HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI
MATEMAATTIS-LUONNONTIETEELLINEN TIEDEKUNTA
MATEMATISK-NATURVETENSKAPLIGA FAKULTETEN
FACULTY OF SCIENCE

Tiedekunta – Fakultet – Faculty	Koulutusohjelma – Utbildningsprogram – Degree programme
Faculty of Science	Mathematics

Tekijä – Författare – Author
Sakari Ikonen

Työn nimi – Arbetets titel – Title
From divisibility and factorization to Iwasawa theory of Zp-extensions

Työn laji – Arbetets art – Level	Aika – Datum – Month and year	Sivumäärä – Sidoantal – Number of pages
M.Sc. thesis	March 2018	49 p.

Tiivistelmä – Referat – Abstract

This thesis covers the factorization properties of number fields, and presents the structures necessary for understanding a proof on Iwasawa's theorem. The first three chapters aim to construct a ring of integers for arbitrary number fields, and prove that such a ring exists.

We prove that our ring of integers is a Dedekind ring, giving us unique factorization on the set of prime ideals. We prove that there exists an isomorphism between principal and factorial divisors and ideals, define an equivalence relation on the set of all divisors, and show that the equivalence classes form the ideal class group. The class number of a field is defined as the order of the ideal class group . We define ramification of primes, and the invariants related to a prime P called the ramification index, inertia degree and decomposition number.

We expand on the galois theory of finite extensions, by introducing a topology on an infinite algebraic galois extension, and a galois correspondence between closed subgroups and intermediate fields. We show how to define the decomposition- and inertia group in the infinite case. The maximal unramified field extension, the Hilbert class field, whose galois group is isomorphic to the ideal class group, is introduced.

We introduce a p-adic metric on the ring of integers with the help of valuations, and construct the p-adic integers as a completion with regards to the metric. We prove some structure results for this ring. The lambda-modules are constructed as a limit of modules over group rings, where the group rings are generated by the p-adic integers, and a suitable multiplicative cyclic group.

The final result is a proof of Iwasawa’s theorem as found in Washington, Introduction to Cyclotomic fields. We view the galois group of the p-adic extension as a lambda-module, and from the structure theorems of lambda-modules, we prove results that carry on to the galois groups of the intermediate fields, culminating in a formula for the exact power of p, that divides the class number of the n-th intermediate field.

Avainsanat – Nyckelord – Keywords
Iwasawa theory, algebraic number theory, class number, unique factorization

Säilytyspaikka – Förvaringställe – Where deposited
Kumpulan tiedekirjasto

Muita tietoja – Övriga uppgifter – Additional information

From divisibility and factorization to Iwasawa theory of $\mathbb{Z}_p$-extensions

Sakari Ikonen
Master's thesis

March 14, 2018

Contents

Chapter 1

Introduction

I have always been interested in the peculiarities of numbers, and different properties of number fields. I recall encountering p-adic extensions for the first time during an introductory course of Galois theory and finding them rather intriguing.

My main goal in this thesis is to further explore the properties of algebraic number fields, starting with how to extend the normal arithmetic properties of $\mathbb{Z}$ to our field extensions. After the arithmetic properties are fleshed out, I study the ideal structures of our ring of integers in the extensions, and thereby hopefully get a grasp on some properties for specific fields, such as p-adic or cyclotomic extensions in regards to factorization over these fields. The final task is to present the proof for Iwasawa's theorem on p-adic extensions, which is a result on the p-part of the class field number of $\mathbb{Z}_p$-extensions.

For some of the more tedious theorems I will point out a source where a proof can be found. It is normal for a proof in the source material to have some steps omitted. In these cases I have filled in the gaps left by the author, to the best of my ability.

My approach to the subjects is with the mindset of a fellow student who is getting familiar with the concepts for the first time, as at the time of writing not many courses on the preliminaries for this subject were being offered. I will be going into more detail on proofs that I found most interesting, and the more tedious ones will be left out due to space constraints. As I have been in a sense working backwards through the subject, starting from my main interest of Iwasawa theory, some of the concepts presented in this thesis might seem a bit disjointed at first. This is the reason why the first half covers divisor theory and valuations extensively, to be able to speak about class numbers for fields and to lay groundwork for later results.

Chapter 2

Preliminaries

I shall assume that the reader has knowledge of the basic results regarding groups, rings and fields so I will focus on covering some of the more advanced preliminary results in this section. The results of this chapter can be found in any general algebra textbook, such as [2], [3] or [9].

Many of our definitions will use a set with an associative operation. This is a bit more general than requiring the set to match group axioms.

Definition 2.1. A set G with a binary operation $\cdot$ is called a *semigroup* if the operation is associative, e.g. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in G$

Definition 2.2. Let K, L be fields and $K \subset L$. We say that L is a *field extension* of K.

Definition 2.3. The *dimension of the extension* L/K is the dimension of L as a K-vector space. We say that L/K is a *finite extension* if its dimension is finite. We denote the degree of the extension as $[L : K] = n$, where $n \in \mathbb{N}$ is the aforementioned dimension.

Definition 2.4. A *number field* is a finite field extension of $\mathbb{Q}$

Definition 2.5. A polynomial P is called *monic* if the coefficient of the variable with the greatest exponent is 1.

Definition 2.6. An element $\alpha \in L$ is called *algebraic* over K if there exists a *monic polynomial* $P(x) \in K[X]$ such that $P(\alpha) = 0$. Specifically, if α is algebraic over $\mathbb{Z}$, we call it an *algebraic integer*.

Theorem 2.7. *For any number field L, there exists an algebraic element $\alpha \in L$ such that $L = \mathbb{Q}(\alpha)$*

Proof. Let $[L : \mathbb{Q}] = n, n \in \mathbb{N}$ be the dimension of L as a $\mathbb{Q}$-vectorspace. Let us choose an element $\alpha \in L$ ($\alpha \neq 0, 1$) and look at the sequence $1, \alpha, \dots \alpha^n \in L$. As L is now a $\mathbb{Q}$-vectorspace of degree n, and we have chosen $n+1$ unique elements, they must be linearly dependent. Therefore there exist elements $a_0, a_1, \dots a_n \in \mathbb{Q}$ such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ and not all a_i are zero. It follows that any element of L is therefore algebraic over $\mathbb{Q}$.

We shall show the existence of a single spanning element by induction on the number of spanning elements. Let $\alpha, \beta \in L$ be algebraic numbers with f and g their respective minimal polynomials. We must show that there exists an element $\lambda \in \mathbb{Q}$ such that $\theta_2 = \alpha + \lambda\beta$ and $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta_2)$. Because a θ_2 defined as such is a linear combination of α and β, it is an element of the field $\mathbb{Q}(\alpha, \beta)$. As such, we have the inclusion $\mathbb{Q}(\theta_2) \subset \mathbb{Q}(\alpha, \beta)$.

Let $\theta_2 = \alpha + \lambda\beta$ with some $\lambda \in \mathbb{Q}$, then $\theta_2 \in L$. Let us define $\phi(x) = f(\theta_2 - \lambda x)$. Then $\phi(\beta) = 0$ so β is a root of the polymonial ϕ. Let us choose λ so that β is the only common root of the polynomials ϕ and g. This is possible, because if there exists a common root $\beta_i \neq \beta$, then $f(\theta_2 - \lambda\beta) = f(\theta_2 - \lambda\beta_i)$, which means that $\theta_2 - \lambda\beta_i = \alpha_i$ where $\alpha_i \neq \alpha$ is some other root. But now we have that $\theta_2 = \alpha + \lambda\beta = \alpha_i + \lambda\beta_i$ so we get the equality

$$\lambda = \frac{\alpha - \alpha_i}{\beta - \beta_i}$$

Because our polynomials f and g have a finite amount of roots, we see that only a finite amount of choices for $\lambda \in \mathbb{Q}$ do not suit our purposes.

Now let λ be chosen as shown possible earlier and let ψ be the minimal polynomial of β in $\mathbb{Q}(\theta_2)$. Then $\psi \mid \phi$ and $\psi \mid g$ because ψ is a minimal polynomial, but $\gcd(\phi, g) = c(x - \beta)$ for some $c \in \mathbb{C}^*$ by our choice of λ, so it follows that $\psi = c(X - \beta) \in \mathbb{Q}(\theta_2)[X]$. This implies that the coefficients c and $c\beta$ belong to the field $\mathbb{Q}(\theta_2)$. As $\mathbb{Q}(\theta_2)$ is a field, it follows that also $c^{-1} \in \mathbb{Q}(\theta_2)$ and because of this, $c^{-1}c\beta = \beta \in \mathbb{Q}(\theta_2)$. But this means that also $\alpha \in \mathbb{Q}(\theta_2)$, because $\theta_2 = \alpha + \lambda\beta \in \mathbb{Q}(\theta_2)$. We have shown that $\alpha, \beta \in \mathbb{Q}(\theta_2)$, and as a field extension, all of their linear combinations are also included, so it follows that $\mathbb{Q}(\alpha, \beta) \subset \mathbb{Q}(\theta_2)$. We conclude that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta_2)$.

For the last part, let us suppose that our claim holds for some algebraic elements $\alpha_1, \alpha_2, \dots, \alpha_n \in L$ so that there exists a $\theta_n \in L$ such that $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_n) = \mathbb{Q}(\theta_n)$. Let an element $\alpha_{n+1} \in L$ be algebraic. It is clear that $\mathbb{Q}(\theta_n) \subset \mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_{n+1})$. As α_{n+1} is algebraic over $\mathbb{Q}$, it is also algebraic over $\mathbb{Q}(\theta_n)$. Because algebraic extensions are the smallest field extensions containing all linear combinations of the spanning elements over the base field, it is apparent that we can write $\mathbb{Q}(\alpha_1, \alpha_2, \dots, \alpha_{n+1}) = \mathbb{Q}(\theta_n, \alpha_{n+1})$. Now we have reduced the problem to two elements, that we have already proven. It follows that there exists a $\theta_{n+1} \in L$ so that $\mathbb{Q}(\theta_n, \alpha_{n+1}) = \mathbb{Q}(\theta_{n+1})$

□

Definition 2.8. By an *integral domain* we mean a commutative ring R where the product $ab = 0$ if and only if $a = 0$ or $b = 0$

Definition 2.9. A *unique factorization domain* (UFD for short) is an integral domain, where factorization into prime elements is unique, up to the order and differing only by a multiple of a unit.

Definition 2.10. For an integral domain R the field of fractions $Quot(R)$ or $Q(R)$ for short, the smallest field consisting of all elements a/b where $a, b \in R$ and $b \neq 0$. It is necessary that the domain does not contain zero divisors, as otherwise we might end up with zero as a denominator for some of our elements.

Definition 2.11. For any commutative rings $R \subset S$ we have the following terminology:

- a element $c \in S$ is *integral* over R if there exists a monic polynomial $f \in R[X]$ satisfying $f(c) = 0$,
- the set $\bar{R}$ of all the integral elements of S over R is called the *integral closure* of R in S, and
- the ring R is said to be *integrally closed* in S if $\bar{R} = R$.

Definition 2.12. Let R be an integral domain and M an Abelian group. We say that M is an R-module if there exists a map $R \times M \to M$ such that for every $r_1, r_2 \in R, m_1, m_2 \in M$

1. $(r_1 + r_2)m_1 = r_1m_1 + r_2m_1$
2. $(r_1r_2)m_1 = r_1(r_2m_1)$
3. $r_1(m_1 + m_2) = r_1m_1 + r_1m_2$
4. $1m_1 = m_1$

Note that here the products between elements of R and M are to be understood as images by the given map, whereas the sums are inside the group M

Lemma 2.13. *Let A be an $n \times n$ matrix. We define the characteristic polynomial for the matrix as $p_A(x) = det(xI - A)$, where I is the identity matrix. The characteristic polynomial is always monic.*

Proof. As A is a square matrix, the determinant is as a sum of permutations as follows,

$$det(xI - A) = \sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} (x_{i,\sigma(i)} - a_{i,\sigma(i)}),$$

where S_n is the symmetric group of a set with n elements. Now we notice that the only elements in the matrix $xI - A$ that contain x are the diagonals $(x - a_{i,i})$ so the greatest term of our polynomial can only be generated by a permutation that picks every diagonal from the matrix, precisely $\sigma(i) = i$ for any $i \leq n$, so $\sigma = id$.

This means that the greatest term of our polynomial is generated by the product

$$sgn(id_n)(x - a_{1,1})(x - a_{2,2}) \dots (x - a_{n,n})$$

First notice that $sgn(id) = 1$ for any size matrix, and now choose from each member of the product x instead of $a_{i,i}$ to generate the greatest power of x, namely x^n. Therefore the leading term of our characteristic polynomial $p_A(x)$ is x^n so it is monic. □

We also need the concept of a group ring for chapters 7 and 8. The idea is simple, when given a group G and a ring R, we construct a module out of these that behaves like a ring. See [16] for specifics.

Definition 2.14. [16] Let G be a multiplicative group and R be a ring. We define the *group ring* of these as

$$R[G] = \{\sum_{g \in G} r_g g \mid r_g \in R, g \in G \text{ and } r_g \neq 0 \text{ only for finitely many } g\}$$

For a proof on $R[G]$ being a ring, and how to define the multiplication of two elements, see [16].

Chapter 3

Ring of integers for algebraic number fields, Divisor theory for domains

The purpose of this section is to expand on our notion of integers for algebraic extensions of $\mathbb{Q}$. Ideally we would like to construct a ring with the common arithmetic properties of $\mathbb{Q}$ and $\mathbb{Z}$, namely unique factorization into primes.

In this chapter, when speaking of a module, we mean a finitely generated subgroup of K^+ of a number field K, which will always be a $\mathbb{Z}$-module.

Definition 3.1. Let K be a number field. We call a ring $\mathfrak{D}$ with the following properties, an *order of* K:

1. $Quot(\mathfrak{D}) = K$
2. $\mathfrak{D} \cap \mathbb{Q} = \mathbb{Z}$
3. The additive group of $\mathfrak{D}$ is finitely generated.

From the second property it follows that $\mathbb{Z} \subset \mathfrak{D}$, and because $\mathfrak{D}$ is a ring, it is closed under multiplication and addition by elements of $\mathbb{Z}$. Combined with the third property this means that any order $\mathfrak{D}$ is a free $\mathbb{Z}$-module.

We must still show that there exists a maximal order $\mathfrak{D}_K$ for a given number field K. We will also show that an element $\alpha \in \mathfrak{D}_K$ if and only if there exists $a_i \in \mathbb{Z}$ such that

$$\alpha^s + a_1\alpha^{s-1} + \cdots + a_n = 0$$

meaning α is an algebraic integer over $\mathbb{Z}$, or sometimes called an integral algebraic number.

Note. Nowadays the notation for the ring of integers is $\mathcal{O}_K$, and $\mathfrak{D}_K$ is used to emphasize that it is a Dedekind ring, which we will define in a later chapter.

Proposition 3.2 ([5]). *Let K be a number field. An algebraic number $\alpha \in K$ is an algebraic integer if and only if there exists a finitely generated $\mathbb{Z}$-module M in K such that $\alpha M \subset M$*

Proof. If α is an algebraic integer, then there exist $r_i \in \mathbb{Z}$ such that

$$1 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} = 0$$

where $n = [K : \mathbb{Q}]$ and we can choose $\{1, \alpha, .., \alpha^{n-1}\}$ as a basis for the module M. By multiplying the elements of the basis of M with α we obtain a basis for αM. It follows that because

$$\alpha(\alpha^{n-1}) = \alpha^n = -\sum_{i=1}^{n-1} r_i\alpha^i \in M$$

then $\alpha M \subset M$.

Conversely if there exists a finitely generated module M such that $\alpha M \subset M$ then if $\beta_1, .., \beta_n$ is a basis for the module, we have for every i some $r_{ij} \in \mathbb{Z}$ that

$$\alpha\beta_i = \sum_{j=1}^{n} r_{ij}\beta_j$$

Let C be the matrix $C = (r_{ij})$, then $(\alpha I - C)(\beta_1, .., \beta_n) = (0, .., 0)$ where I is the identity matrix, which means that α is the eigenvalue and $(\beta_1, \ldots, \beta_n)$ the eigenvector of the matrix C. Therefore the matrix $\alpha I - C$ is not invertible, and α is a root of the characteristic polynomial $det(xI - C) \in \mathbb{Z}[X]$. As the characteristic polynomial of a square matrix is always monic (see Lemma 2.13), α is an algebraic number. □

Definition 3.3. Let M be a *complete* module in a number field K, in other words $rank(M) = [K : \mathbb{Q}]$. We call

$$\mathfrak{D}(M) = \{\alpha \in K \quad | \quad \alpha M \subset M\}$$

the *order of M*.

Proposition 3.4. *Let M be a complete module in K. Then $\mathfrak{D}(M)$ is an order in K. For every order D there exists a complete module M such that $D = \mathfrak{D}(M)$.*

Proof. By definition and Proposition 3.2, it follows that every element of $\mathfrak{D}(M)$ is an algebraic integer, so $\mathfrak{D}(M) \cap \mathbb{Q} = \mathbb{Z}$. Any order for a number field $K = \mathbb{Q}(\alpha)$ must contain α, otherwise K will not be the quotient field.

□

Theorem 3.5 ([5]). *Let K be a number field and $\mathfrak{D}_K$ be the set of all algebraic integers of K. Then $\mathfrak{D}_K$ is the maximal order of K.*

Proof. Let $\alpha, \beta \in K$ be algebraic integers, then by Proposition 3.2 there exist $\mathbb{Z}$-modules M_1, M_2 for which $\alpha M_1 \subset M_1$ and $\beta M_2 \subset M_2$. Let $(\alpha_1, \ldots, \alpha_n)$ be a basis for M_1 and $(\beta_1, \ldots, \beta_m)$ a basis for M_2. Then

$$\{\alpha_i \beta_j \quad | \quad 1 \leq i \leq n, 1 \leq j \leq m\}$$

is a basis for the $\mathbb{Z}$-module $M_1 M_2$, which is a product of two modules. From Proposition 3.2 it follows that $(\alpha \pm \beta) M_1 M_2 \subset (\alpha M_1) M_2 + M_1(\beta M_2) \subset M_1 M_2$ and $(\alpha\beta) M_1 M_2 \subset (\alpha M_1)(\beta M_2) \subset M_1 M_2$. Therefore $\mathfrak{D}_K$ is a ring.

Let $M \subset K$ be a complete module contained in $\mathfrak{D}_K$, such a module exists based on proposition 3.4 as we can choose any $\delta \in \mathfrak{D}_K$ and use the complete module M corresponding to the order $\mathfrak{D}(M_\delta)$. If $M \neq \mathfrak{D}_K$ then choose $\alpha_1 \in \mathfrak{D}_K - M$ and let (M, α_1) be the module generated by M and α_1 in K. Now if $(M, \alpha_1) \neq \mathfrak{D}_K$ we choose $\alpha_2 \in \mathfrak{D}_K - (M, \alpha_1)$ and continue. Because K has a finite basis as a number field, it follows that this process will complete after a finite amount of steps, and we are left with a module $(M, \alpha_1, \ldots, \alpha_i) = \mathfrak{D}_K$. □

Divisor theory for domains

From this point onward if necessary, we are going to use the term *rational integer* to emphasize that our integer belongs to $\mathfrak{D}_\mathbb{Q} = \mathbb{Z}$.

Example 3.6. Let us consider the extension $\mathbb{Q}(\sqrt{-7})$ (in fact any Gaussian rational extension will do!). We will notice that just considering arithmetic as unique factorization into prime elements is not enough, as now the number 8 has two different representations, namely 2^3 and $(1 + \sqrt{-7})(1 - \sqrt{-7})$

Ideally we would want some method to group up different representations of the same elements. This is the motivation for the following definition, where we utilize the existing Order for a given domain.

Definition 3.7. Let R be a domain and $\mathfrak{D}$ a free abelian semigroup. We define a *divisor theory* for the domain R with a given homomorphism $f : R^* \to \mathfrak{D}$ where $R^* = (R \setminus \{0\}, \cdot)$ with the properties that

1. $a \in R^*$ divides $b \in R^*$ if and only if $f(a)$ divides $f(b)$. $\alpha \in \mathfrak{D}$ divides $a \in R$ if $a = 0$ or α divides $f(a)$. When a divides b we write it as $a \mid b$ and when α divides a we extend our usual notation, and write $\alpha \mid a$.

2. if $\alpha \in \mathfrak{D}$ divides $a, b \in R$ then α divides $a \pm b$

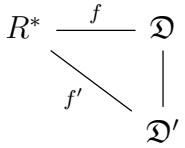
3. if $\{a \in R \mid \alpha | a\} = \{b \in R \mid \beta | b\}$, then $\alpha = \beta$

Our definition is more general than necessary, so it is worth noting that a free abelian semigroup is automatically a unique factorization domain, which gives us the property we are after.

Note. We call the elements of the semigroup $\mathfrak{D}$ the divisors of R. Naturally the elements that are prime in $\mathfrak{D}$ are called *prime divisors*. The elements $\alpha \in \mathfrak{D}$ for which $\alpha \in Im(f)$ are called the *principal divisors*.

For such a definition to be meaningful, we need to be sure that it is well-defined. The first problem that comes to mind is if we could have two distinct divisor theories for a given domain. The next theorem shows that this is not the case, and that all divisor theories for a given domain are essentially the same.

Theorem 3.8. *[4] If $f : R^* \to \mathfrak{D}$ and $f' : R^* \to \mathfrak{D}'$ are two divisor theories of R, then there exists a unique isomorphism $\mathfrak{D} \cong \mathfrak{D}'$ for which the following diagram commutes.*



Proof. Let f, f' be the two divisor theories for R. Let $p \in \mathfrak{D}$ and $p' \in \mathfrak{D}'$ be prime divisors. Lets denote by $\bar{p}$ and $\bar{p}'$ the sets of elements of R that are divisible by p and p' respectively.

First, let us show that for any prime divisor $p' \in \mathfrak{D}'$ there exists a prime divisor $p \in \mathfrak{D}$ such that $\bar{p} \subset \bar{p}'$. To do this, suppose that for all prime divisors $p \in \mathfrak{D}$ it holds that $\bar{p} \not\subset \bar{p}'$. From property (3) of the divisor theory, we have that

$$\{a \in R \mid p' \mid a\} \neq \{0\}$$

Choose an element $b \in R, b \neq 0$ that is divisible by p' and then decompose $f(b) \in \mathfrak{D}$ into prime factors of $\mathfrak{D}$. Doing so we get

$$f(b) = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$

where every p_i is a prime factor in $\mathfrak{D}$.

Because we assumed $\bar{p} \not\subset \bar{p}'$ then for any $i = 1, \dots, n$ there exists an element $\gamma_i \in R$ which is divisible by p_i but not by p', because $\bar{p}_i$ is not just an empty set. But now the product

$$\gamma = \gamma_1^{k_1} \gamma_2^{k_2} \dots \gamma_n^{k_n}$$

is divisible by $f(b)$. From property (1) of our divisor theory we have that $f(b) \mid \gamma$ if and only if $\gamma = 0$, or $f(b)$ divides $f(\gamma)$. Trivially, $\gamma \neq 0$. Likewise by property (1) we have that because p_i divides γ_i for any i, it follows that $f(p_i) \mid f(\gamma_i)$. But this means that our element $b \in R$ divides $\gamma \in R$. Recall that we chose b to be divisible by p', but now because b divides γ, it follows that p' also divides γ. This is a contradiction to our original assumption. Thus for any prime divisor $p' \in \mathfrak{D}'$ there exists a prime divisor $p \in \mathfrak{D}$ such that $\bar{p} \subset \bar{p}'$.

By symmetry, for any $p \in \mathfrak{D}$ there exists a $q' \in \mathfrak{D}'$ so that $\bar{q}' \subset \bar{p}$. Next we want to show that $q' = p'$, from which it follows that $\bar{p}' = \bar{p}$. We started off by choosing for a given $p' \in \mathfrak{D}'$, a $p \in \mathfrak{D}$ so that $\bar{p} \subset \bar{p}'$. Next we choose a $q' \in \mathfrak{D}'$ so that we have the inclusion $\bar{q}' \subset \bar{p} \subset \bar{p}'$

By condition (3) the following holds true

$$\{a \in R \mid q' \mid a\} \subset \{a \in R \mid q'p' \mid a\}$$

So let $\zeta \in R$ be an element divisible by q' and not by $q'p'$. Assume $q' \neq p'$. Because ζ is not divisible by $q'p'$ but is divisible by q' it follows that ζ is not divisible by p'. This is a contradiction because $\bar{q}' \subset \bar{p}'$. Therefore $\bar{p}' = \bar{p}$.

We have shown that for any prime divisor $p' \in \mathfrak{D}'$ there exists a prime divisor $p \in \mathfrak{D}$ so that $\bar{p} = \bar{p}'$. From property (3) of our divisor theory it follows that because the sets are equal, the element p is uniquely defined.

This unique representation can be generalized to all prime divisors, generating an isomorphism $\mathfrak{D} \cong \mathfrak{D}'$ by defining a map between prime factor counterparts as $p_i \leftrightarrow p_i'$, and more generally

$$p_1^{k_1} \dots p_n^{k_n} \leftrightarrow p_1'^{k_1} \dots p_n'^{k_n}$$

where $p_i \in \mathfrak{D}$ and $p_i' \in \mathfrak{D}'$

Next we need to show that for a given $a \in R$ the divisors of $f(a) \in \mathfrak{D}$ and $f'(a) \in \mathfrak{D}'$ correspond to each other. Let $p \in \mathfrak{D}$ and $p' \in \mathfrak{D}'$ be matching prime divisors that occur in the factorization of $f(a)$ and $f'(a)$, with exponents k and m respectively. From condition (3) we have that there exists an element $\beta \in R$ that divides p but not p^2 because $p \neq p^2$ so their divisor sets are not the same either. Since $\bar{p} = \bar{p}'$, p' also divides β.

The principal divisor $f(\beta)$ therefore has the form

$$f(\beta) = pd, \quad d \in \mathfrak{D}$$

where d is not divisible by p. Now lets choose in the same manner as we did with β, an element $\gamma \in R$ so that it is divisible by d^k but not by pd^k. Since p does not divide d, it does not divide d^k either, and because of this, γ is not divisible by p or p'.

Let us go back to our original $a \in R$ now and examine the product $a\gamma$. Because a is divisible by p^k and γ is divisible by d^k, the product $a\gamma$ is divisible by $p^k d^k = f(\beta^k)$. As

such, from condition (1) it follows that

$$a\gamma = \beta^k c \quad c \in \mathfrak{D}$$

Now recall that also $p' \mid \beta$ so $a\gamma$ is divisible by p'^k. Because we chose γ to be not divisible by p', it follows that $p'^k \mid a$. This means that for the exponent of p' in the factorization of $f'(a) \in \mathfrak{D}'$ that we denoted as m, it holds that $m \geq k$. By symmetry we also prove that $k \geq m$.

Finally we have the result, that for a factorization $f(a) = p_1^{k_1} \dots p_n^{k_n}$ with our isomorphism $\mathfrak{D} \cong \mathfrak{D}'$

$$f'(a) = p_1'^{k_1} \dots p_n'^{k_n}$$

which means that the principal divisors $f(a)$ and $f'(a)$ correspond to each other and our original diagram commutes. □

The second problem we have with our divisor theory definition, is the existance of one. What guarantee do we have that a divisor theory even exists for a domain. The next theorem will give a necessary condition in the case of a unique factorization domain. Note that this does not cover all of our bases, as seen in the example 3.6.

Theorem 3.9. *[4] A domain R is a UFD(Unique Factorization Domain) if and only if R has a divisor theory with which all divisors are principal divisors.*

Proof. If the ring R is a UFD, then for a given element $a \in R^*$ lets consider all the elements $b \in R^*$ that are associates of a, meaning $b = ar$ for some unit $r \in R$. Let

$$f : R^* \to \mathfrak{D}$$

be defined as $f(a)$ being the set of all the elements of R that are associates of a, and the set $\mathfrak{D}$ as the set of all such associate classes. For $a, b \in R^*$ lets define multiplication by

$$f(a)f(b) = f(ab)$$

Let us first check if f is well defined. Let $a' \in f(a)$ and $b' \in f(b)$, then $a' = ar_a$ and $b' = br_b$ for some units $r_a, r_b \in R$. As we assumed our ring to be a UFD, it is an integral domain, and thus is commutative, we get

$$\begin{aligned} a'b' &= ar_a br_b \\ &= abr_a r_b \\ &= abr_{ab} \end{aligned}$$

where r_{ab} is the product of the two units r_a, r_b, which is also a unit. Therefore $a'b' \in f(ab)$, and we conclude that the product we defined does not depend on the choice of representatives. By this definition and because R is a ring with commutative multiplication, the following equalities hold $f(a)(f(b)f(c)) = f(a)f(bc) = f(abc) = (f(a)f(b))f(c)$. We clearly see that $\mathfrak{D}$ is a semigroup with our definition of multiplication.

Let us check if f is also a valid divisor theory for R.

For the first requirement, for $a, b \in R^*$, $a \mid b$ means $b = ar$ for some $r \in R^*$. Then $f(b) = f(ar) = f(a)f(r)$ so it is also true that $f(a) \mid f(b)$. And the other way around, if $f(a) \mid f(b)$, then $f(b) = f(a) \cdot \gamma$ for some $\gamma \in \mathfrak{D}$. Because $\mathfrak{D}$ only consists of associate classes, there must be a representative for the class γ, so assume that $f(r) = \gamma$ for some $r \in R^*$. Now we have the equality $f(b) = f(a)f(r) = f(ar)$, which means that the associates of b and ar are the same, therefore $a \mid b$.

For the second requirement, let $\alpha \in \mathfrak{D}$ divide $a, b \in R$. Notice that if $c \in f(a+b)$, then $c = (a+b)r$ for an unit $r \in R^*$. But then $c = ar + br$, which would mean that $c \in f(a) + f(b)$. Therefore α divides $f(a+b)$ as well.

For the third requirement, let $\alpha, \beta \in R$ and suppose

$$\{a \in R \mid \alpha \mid a\} = \{b \in R \mid \beta \mid b\}$$

then if $\alpha \mid a$, it also holds that $\beta \mid a$, and we get $\alpha a' = \beta b'$. The equality holds only if $\alpha = \beta$, as we assumed our domain to be a UFD.

For the converse, let us assume that we have a ring R and a divisor theory $f : R^* \to \mathfrak{D}$ such that all divisors are principal divisors. Let $p \in R$ and $f(p)$ be the corresponding principal divisor in $\mathfrak{D}$. We shall prove our original claim by proving that a principal divisor of $\mathfrak{D}$ is prime if and only if the corresponding element in R is prime.

First, if $f(p) = \alpha$ is prime in the semigroup $\mathfrak{D}$, then for any $b \in R$ that divides p, $f(b)$ divides α. Because α is prime, $f(b) = \alpha$ or $f(b) = 1$. In the case of $f(b) = \alpha$ it means that b is an associate of p, so $p = be$ for a unit e, and in the case of $f(b) = 1$ it means that b is an unit of R. From this it follows that our $p \in R$ is a prime element, because it is only divisible by its associates and the units of the ring. If an element $f(b) = \beta$ is neither prime, nor a unit, then there exists a prime divisor $f(p) = \alpha$ so that $\alpha \mid \beta$. The element $p \in R$ exists because we assumed all our divisors were principal. The first property of a divisor theory gives us the implication that $\alpha \mid \beta \Rightarrow p \mid b$, which means that b is divisible by a prime element it is not associates with, therefore b is not prime. We now have the useful result that

$$p \in R \text{ is prime} \Leftrightarrow f(p) \in \mathfrak{D} \text{ is prime}$$

Finally lets consider factorization in R. For an element $a \in R$ let

$$f(a) = \alpha_1 \alpha_2 \dots \alpha_n$$

be the factorization in $\mathfrak{D}$, with prime divisors α_i. As proven before, there must exist primes $p_i \in R^*$ so that $f(p_i) = \alpha_i$ for $i \leq n$. Because f is a divisor theory, and thus a homomorhism, we have

$$f(a) = f(p_1)f(p_2)\dots f(p_n) = f(p_1p_2\dots p_n)$$

which again, means that a and the product of primes $p_1p_2\dots p_n$ are associates, therefore

$$a = ep_1p_2\dots p_n$$

where e is a unit of R. Since the factorization in $\mathfrak{D}$ is unique up to permutations, and because as shown, the factorization in $\mathfrak{D}$ induces a factorization in R, it follows that R is a UFD. □

Our ultimate goal is to show that a divisor theory exists for a maximal order $\mathfrak{D}_K$ of an algebraic number field. The next theorem tells to us that we can construct a divisor theory only for the maximal order.

Theorem 3.10. *[5][4] If a domain R has a divisor theory, then R is integrally closed.*

Proof. Let $f : R \to \mathfrak{D}$ be the divisor theory in question. Let $\gamma \in Quot(R)$ be an element such that $\gamma \notin R$ and that there are elements $a_1, \dots, a_n \in R$ so that

$$\gamma^n + \gamma^{n-1}a_1 + \dots + a_n = 0 \tag{3.11}$$

Let $\gamma = a/b$ with $a, b \in R$ and $b \nmid a$, otherwise $\gamma \in R$. Then by our divisor theory $f(b) \nmid f(a)$ also. From this it follows that there exists a prime divisor $p \in \mathfrak{D}$ so that $p \mid f(b)$ and the exponent of p in the factorization $f(b)$ is greater than that of $f(a)$. Let the integer k be the exponent, with which the factor p occurs in $f(a)$. Then $p^{k+1} \mid f(b)$ and $p^{k+1} \nmid f(a)$. Let us consider the following equation, that we get from 3.11 by substituting $\gamma = a/b$

$$a^n = -a_1a^{n-1}b - a_2a^{n-2}b^2 - \dots - a_nb^n$$

All the products $a^{n-i}b^i$ on the right side of the equation are divisible by p at least $k(n-i) + (k+1)i = kn + 1$ times, therefore the right side of the equation is divisible by p^{kn+1}. The left side of the equation consists only of a^n, and we chose p to divide a only k-times, therefore $p^kn \mid a^n$ but $p^{kn+1} \nmid a^n$. This contradicts our assumption that $\gamma \notin R$ and we conclude that every element of $Quot(R)$ that is integral over R, must be in R, therefore R is integrally closed. □

We still need to prove the existence of a divisor theory for our ring of integers $\mathfrak{D}_K$. We are going to be proving this with the valuation theoretic approach, as valuations play

a key role in studying other properties of fields in modern algebra, and the concept of valuations will be useful in later chapters as well. Our main result is going to be that a set of all valuations on a field K induces a divisor theory for the ring of integers.

First, we define what we mean by a valuation

Definition 3.12. Let K be a field. We say that a function $v : K \to \mathbb{Z} \cup \{\infty\}$ is a valuation of the field K, if the following properties are satisfied:

1. v is surjective and $v(0) = \infty$,
2. $v(\alpha\beta) = v(\alpha) + v(\beta)$ for all $\alpha, \beta \in K$, and
3. $v(\alpha + \beta) \geq min(v(\alpha), v(\beta))$ for all $\alpha, \beta \in K$.

Note. In some cases we can strengthen the third property in our definition, for any $\alpha, \beta \in K$ if $v(\alpha) \neq v(\beta)$ then assuming $v(\alpha) > v(\beta)$ it also holds that because $\beta = (\alpha + \beta) - \alpha$ then

$$\begin{aligned} v(\beta) &\geq min(v(\alpha + \beta), v(-\alpha)) \\ &= min(v(\alpha + \beta), v(\alpha)) \end{aligned}$$

as $v(-\alpha) = v(-1) + v(\alpha) = v(\alpha)$ by the second property. Combining this inequality and our assumption we get

$$v(\alpha) > v(\beta) \geq v(\alpha + \beta)$$

and this shows that $v(\alpha + \beta) \leq min(v(\alpha), v(\beta))$.

With this we have proven the very useful equality

$$v(\alpha + \beta) = min(v(\alpha), v(\beta)) \quad \text{for } v(\alpha) \neq v(\beta)$$

We will need this in some later proofs in this chapter.

Example 3.13. As an example of a valuation, for a given prime divisor p, we can define $v_p(\alpha)$ as being the power of p in the factorization of α. If p is not a factor, then $v_p(\alpha) = 0$.

Proof. For the first property, first note that $v_p(0) = \infty$ because we can divide 0 by a prime p as many times we like. As p and p^2 are distinct divisors, there exists an element γ that is divisible by p and not by p^2, thus $v_p(\gamma) = 1$. This also means that $v_p(\gamma^k) = k$ for any integer k, so our valuation exhausts $\mathbb{Z}$ as required.

For the second property, if α has p^k and β has p^m as factors, then $\alpha\beta$ has $p^k p^m = p^{k+m}$ as a factor, and we observe that the second property holds true.

For the third property, if p is such a factor in α and β that for some i it holds that $p^{i+1} \mid \alpha$ but $p^{i+1} \nmid \beta$, but for any exponent $k < i + 1$ the factor p^k divides both, then it

follows from divisibility axioms that also the sum $\alpha + \beta$ is divisible by p^k. This shows that the inequality of the third property holds true.

Especially worthy of mentioning are the p-adic valuations on $\mathbb{Q}$ that are constructed in this way. For example the 5-adic valuation v_5 would yield

$$v_5(\frac{6}{25}) = -2 \quad \text{and } v_5(20) = 1$$

□

The valuation in Example 3.13 can be extended to the quotient field of the ring $\mathfrak{D}$ by defining

$$v_p(\gamma) = v_p(\alpha) - v_p(\beta) \quad \text{for } \gamma = \alpha/\beta \quad \alpha, \beta \in \mathfrak{D}$$

Our first theorem concerning valuations is going to give necessary conditions for the set of all valuations to induce a divisor theory on a given ring $\mathfrak{D}$

Theorem 3.14. *[4] Let $\mathfrak{D}$ be a ring with a quotient field K and let $\mathfrak{R}$ be the set of valuations of K. In order for the valuations in $\mathfrak{R}$ to induce a divisor theory on $\mathfrak{D}$, it is necessary and sufficient that these conditions hold.*

1. *for any $\alpha \in \mathfrak{D}$, if $\alpha \neq 0$ then it holds that $v(\alpha) = 0$ for almost all valuations $v \in \mathfrak{R}$,*
2. *$\alpha \in K$ belongs to $\mathfrak{D}$ if and only if $v(\alpha) \geq 0$ for all $v \in \mathfrak{R}$, and*
3. *for any finite set of distinct valuations $v_1, \ldots v_n \in \mathfrak{R}$ and for any set of nonnegative integers $z_1, \ldots, z_n$ there is an element $\alpha \in \mathfrak{D}$ for which $v_1(\alpha) = z_1, \ldots, v_n(\alpha) = z_n$*

Going forward, when we use the phrase *for almost all*, we mean *for all but a finite number of.*

Proof. We shall first characterize the principal divisors with the help of our valuations. Define a function

$$f(\alpha) = \prod_p p^{v_p(\alpha)} \quad \alpha \in \mathfrak{D}^* \tag{3.15}$$

where p goes through all prime divisors satisfying $v_p(\alpha) > 0$. Now we see that the valuations induce a homomorphism and the semigroup D as soon as the set of prime divisors is known.

Lets start by verifying the first property. Let $\alpha \in \mathfrak{D}, \alpha \neq 0$. For a valuation $v \in \mathfrak{R}$ the factorization of the principal divisor $f(\alpha)$ of the form 3.15 contains only a finite number of factors, so only a finite amount of valuations satisfy $v(\alpha) > 0$.

For the second property, we first note that for all $\alpha \in \mathfrak{D}$ it holds that $v(\alpha) \geq 0$ because either α has p as a factor, or it does not. Conversely, assume that for some $\gamma \in K, \gamma \neq 0$ it holds that $v(\gamma) \geq 0$ for all valuations $v \in \mathfrak{R}$. Let $\gamma = \alpha/\beta$ with $\alpha, \beta \in \mathfrak{D}$.

Then $v(\gamma) = v(\alpha) - v(\beta) \geq 0$, so $v(\alpha) \geq v(\beta)$ for all valuations $v \in \mathfrak{R}$. But this means that $f(\alpha)$ is divisible by $f(\beta)$, which implies that $\beta \mid \alpha$. But then $\gamma \in \mathfrak{D}$, which is a contradiction.

Now to verify the third and last property. Let $v_1, \ldots, v_n \in \mathfrak{R}$ be a finite set of valuations, which correspond to prime divisors $p_1, \ldots, p_n$. Let $z_1, \ldots, z_n$ be nonnegative integers. We first define a helpful divisor

$$a = p_1^{z_1} p_2^{z_2} \ldots p_n^{z_n}$$

Next we define for every $1 \leq i \leq n$ an element

$$a_i = a p_1 p_2 \ldots p_{i-1} p_{i+1} \ldots p_n$$

Now as the elements a_i and $a_i p_i$ are distinct, by the properties of divisor theories there exists for each i an element α_i that is divisible by a_i but not by $a_i p_i$. Now lets consider the sum of such elements, denoted as

$$\alpha = \alpha_1 + \cdots + \alpha_n$$

For a valuation $v_i(\alpha)$ we now check for each α_i against the valuation and note that α_i is divisible by $p_i^{z_i}$ and not by $p_i^{z_i+1}$, hence this applies to the sum also. This means that $v_i(\alpha) = z_i$ for all $1 \leq i \leq n$.

We have shown that our conditions are necessary, if the ring $\mathfrak{D}$ has divisor theory. We must still check that they are also sufficient, and that our construction actually induces a divisor theory on the ring.

For this, let D be a semigroup with unique factorization, and the prime elements of D in a one-to-one relation to the valuations of $\mathfrak{R}$. Denote by v_p the valuation $v \in \mathfrak{R}$ that corresponds to the prime p. The map $f : \mathfrak{D}^* \to D$ defined by 3.15 is a homomorphism, since, by the properties of valuations,

$$f(\alpha\beta) = \prod p_i^{v_{p_i}(\alpha\beta)} = \prod p_i^{v_{p_i}(\alpha)+v_{p_i}(\beta)} = \prod p_i^{v_{p_i}(\alpha)} \prod p_i^{v_{p_i}(\beta)} = f(\alpha)f(\beta) \tag{3.16}$$

From the above equality we also observe that $\beta \mid \alpha$ if and only if $v(\alpha) \geq v(\beta)$ for all $v \in \mathfrak{R}$. Thus our map satisfies the first condition of a divisor theory.

The second condition for a divisor theory is simple, as if for some prime p, $p \mid f(\alpha)$ and $p \mid f(\beta)$ means that $v_p(\alpha) = k$ and $v_p(\beta) = l$ for some nonnegative integers k, l. From the properties of valuations, we have that

$$v_p(\alpha \pm \beta) \geq min(v_p(\alpha), v_p(\beta))$$

hence p also divides $\alpha \pm \beta$

For the third condition for divisor theories, let $a \neq b$, $a, b \in \mathfrak{D}$ and a prime p such that occurs in their factorization with exponents k, l respectively. Assume $k < l$. As we have proven, there exists an element $\alpha \in \mathfrak{D}$ for which $v_p(\alpha) = k$ and that is divisible by a. It follows that our α can not be divisible by b as well, because we run out of factors. This means that the sets $\{\alpha \in \mathfrak{D} \mid a \mid \alpha\}$ and $\{\beta \in \mathfrak{D} \mid b \mid \beta\}$ are the same only if $a = b$

We have proven that the map f in (3.15) induced by the valuations is a divisor theory. □

For a given valuation v, there is a very natural set we can define, namely the set of all the elements in a field for which the valuation gives a nonnegative value. We shall first prove one property for this set, before giving a formal definition. Afterwards we will prove one useful property of the set.

Proposition 3.17. *[4] Let v be a valuation of a field K. Define a set for the valuation as*

$$D_v = \{\alpha \in K \mid v(\alpha) \geq 0\}$$

The set D_v is a ring.

Proof. As the underlying elements used for D_v are part of a field, we only need to check if the set is closed under sum and multiplication, and if it contains the necessary neutral elements.

Let $\alpha, \beta \in D_v$. Then based on the properties of valuations, we have

$$v(\alpha\beta) = v(\alpha)v(\beta) \geq 0$$
$$\text{and } v(\alpha \pm \beta) \geq min(v(\alpha), v(\beta)) \geq 0,$$

so we note that also $\alpha \pm \beta \in D_v$ and $\alpha\beta \in D_v$.

By definition, for any valuation $v(0) = \infty$. Also $v(\pm 1) = 0$, so the neutral elements $0, 1 \in D_v$ as well. □

Definition 3.18. The set D_v is called the (discrete) *ring of the valuation v*. We call the elements of D_v *integral in relation to the valuation v*.

Lemma 3.19. *[4] Let v be a valuation of a field K. The ring D_v is integrally closed in K.*

Proof. We start by proving that the ring D_v has a divisor theory.

Let $\mathfrak{R} = \{v\}$. Now we can confirm the necessary conditions outlined in Theorem 3.14. By our definition of D_v, for any $\alpha \in D_v$, $v(\alpha) \geq 0$ for in this case, all valuations in $\mathfrak{R}$.

Since v is the generating valuation for the ring D_v, then $\alpha \in D_v$ if and only if $v(\alpha) \geq 0$ for all, or in our case the only one $v \in \mathfrak{R}$.

Let $v \in \mathfrak{R}$ and z_1 be a nonnegative integer. Because v is a valuation, then it must be true that $v(\alpha) = z_1$ for some $\alpha \in K$, because as a valuation, $v(K) = \mathbb{Z} \cup \{\infty\}$. As $z_1 \geq 0$, we have that $\alpha \in D_v$.

Based on Theorem 3.14, our ring D_v has a theory of divisors induced by the set $\mathfrak{R} = \{v\}$. By Theorem 3.10 we know that D_v is integrally closed in its quotient field. As all the elements of D_v also belong to K, then the following applies for the quotient field $Q(D_v) \subset K$. Thus D_v is integrally closed in K as well. □

Now that we have a ring structure induced by our valuation v, we might find it useful to study the ideals of the ring D_v. Especially useful would be to define a maximal ideal I, as then the quotient D_v/I would become a field. The next lemma gives a definition for this maximal ideal.

Lemma 3.20. *[4] Let v be a valuation for a field K, and let D_v be the valuation ring of v. Then the set*

$$I_v = \{\alpha \in K \mid v(\alpha) > 0\}$$

is a maximal ideal of the ring D_v.

Proof. First we check that I_v is an ideal of D_v. Let $\alpha, \beta \in I_v$ and $\gamma \in D_v$. Then from the properties of valuations we have that

$$\begin{aligned} v(\alpha\gamma) &= v(\alpha) + v(\gamma) > 0 \\ \text{and } v(\alpha - \beta) &\geq min(v(\alpha), v(-\beta)) \\ &= min(v(\alpha), v(\beta)) > 0, \end{aligned}$$

so $\alpha\gamma \in I_v$ and $\alpha - \beta \in I_v$. This means that I_v is an ideal of D_v.

Next we assume that I_v is not maximal. Then let $I_v \subset I \subset D_v$ be a greater ideal. Let $\alpha \in I \setminus I_v$. Then $v(\alpha) \leq 0$, but as $\alpha \in D_v$ also, it means that $v(\alpha) = 0$. As K is a field, α^{-1} exists and by the properties of valuations $v(\alpha^{-1}) = -v(\alpha) = 0$ so $\alpha^{-1} \in D_v \setminus I_v$. But then $v(\alpha\alpha^{-1}) = v(1) = 0$ because I is an ideal, so $1 \in I$ which means $I = D_v$. Therefore I_v is maximal. □

With the help of our valuation ring, and the aforementioned maximal ideal, we can now define a field with their quotient as follows.

Definition 3.21. Let v be a valuation of a field K. The ring of the valuation D_v and its maximal ideal I_v form a field

$$K_v = D_v/I_v$$

called the *residue class field of v*.

As our goal for our valuations is to ultimately leapfrog between fields in field extensions, thus transferring properties from the base field to the extension, we want to rigorously define what we mean by an extension of a valuation v of a field K into a finite field extension L. The definition might seem very backwards compared to the way undergraduate mathematicians are used to extending functions. We are going to approach the problem by restricting an existing valuation in the bigger field L. This is the motivation for the following lemma.

Lemma 3.22. *[4] For a finite extension L of a field K, and a valuation v of the field L, there exists an element $e \in K^*$ so that*

$$v_0(\alpha) = \frac{v(\alpha)}{e} \quad \text{for } \alpha \in K^*, \text{ and } v_0(0) = \infty$$

is a valuation for K.

Proof. The problem with simply restricting a valuation v of L to K is that our valuation might not exhaust $\mathbb{Z}$ with just the elements of K, therefore the first property of valuations might not necessarily hold true. However, $v(K) \neq \{0\}$, because otherwise we would have $K \subset D_v$, and as D_v is integrally closed in L as shown by Theorem 3.19, this would mean that for any $f \in D_v[X]$

$$f(\alpha) = 0 \Leftrightarrow \alpha \in L$$

especially for any $f \in K[X]$, and as such the field L would be contained in D_v as well, but this is impossible.

For $\alpha \in K^*$, $v(\alpha)$ takes on positive and negative values, because over a field, the following is true for valuations

$$\begin{aligned} 0 &= v(1) = v(\alpha/\alpha) \\ 0 &= v(\alpha) + v(\alpha^{-1}) \\ v(\alpha) &= -v(\alpha^{-1}) \end{aligned}$$

As the values of $v(K)$ form an ordered set, there is a smallest positive value $e \in v(K)$, and we can denote by some $p \in K^*$ the element for which $v(p) = e$.

Now for any $\alpha \in K^*$, if $v(\alpha) = n$ is not divisible by e, then $n = me + r$ for some $0 \leq r < e$, but as such, then

$$\begin{aligned} v(\alpha p^{-m}) &= v(\alpha) + v(p^{-m}) \\ &= n - me \\ &= me + r - me = r \end{aligned}$$

But now we notice that, as $\alpha p^{-m} \in K^*$ and we chose $v(p)$ to be the minimal positive value, then $r = 0$ and this means that $e \mid n$

We can now set

$$v_0(\alpha) = \frac{v(\alpha)}{e} \quad \text{for } \alpha \in K^*$$

as e is positive, it is natural to also define $v_0(0) = \infty$ because for our original valuation $v(0) = \infty$. For the first property of valuations, we note that for our previous chosen p, it now holds that

$$v_0(p^z) = \frac{v(p^z)}{e} = \frac{zv(p)}{e} = z$$

for any rational integer z. Thus v_0 fulfills the first property.

The second and third property hold true as a consequence of v being a valuation. For $\alpha, \beta \in K^*$, we have

$$v_0(\alpha\beta) = \frac{v(\alpha\beta)}{e} = \frac{v(\alpha) + v(\beta)}{e} = \frac{v(\alpha)}{e} + \frac{v(\beta)}{e} = v_0(\alpha) + v_0(\beta)$$

and

$$v_0(\alpha \pm \beta) = \frac{v(\alpha \pm \beta)}{e} \geq \frac{min(v(\alpha), v(\beta))}{e} = min(\frac{v(\alpha)}{e}, \frac{v(\beta)}{e}) = min(v_0(\alpha), v_0(\beta)).$$

Therefore our constructed v_0 is a valuation of the field K. □

Definition 3.23. Let L be a finite field extension of a field K. Let v be a valuation of L, and let v_0 be the valuation constructed in Lemma 3.22. We say that v is an extension of v_0 into L.

As we plan on using extensions of v_0 to prove things on the field extension L, we must first ask the question if v_0 has any extensions to begin with, and if so, how many are there? The next three theorems explore this problem.

Theorem 3.24. *[4] If $v_1, \ldots, v_m$ are distinct valuations of a field K, then for any rational integers $z_1, \ldots, z_m$ there exists an element $\gamma \in K$ so that $v_1(\gamma) = z_1, \ldots, v_m(\gamma) = z_m$.*

Proof. We shall prove this by induction on the number of valuations. Denote this number by m.

If $m = 1$, then by our definition of a valuation, $v(K) = \mathbb{Z}$, so the claim is true.

Now assume $m \geq 2$ and that our claim holds for sets with at most $m - 1$ valuations.

For our theorem to be true, it would mean that given our set of valuations, we can find an element $\gamma \in K$ to produce an arbitrary set of rational integers. This means that for the equation

$$c_1 v_1(\gamma) + c_2 v_2(\gamma) + \cdots + c_m v_m(\gamma) = 0 \tag{3.25}$$

we can not find rational integer coefficients c_i so that the equation holds for all $\gamma \in K$, because the valuations dont just cycle between a finite set of values.

Let us assume the converse, that instead, equation (3.25) holds for all $\gamma \in K$ with some rational integer coefficients c_i. Then at least two of these coefficients must be nonzero and of the same sign, as otherwise we would have two coefficients c_1, c_2 with $c_1 > 0$ and $c_2 < 0$ and from this it would follow that

$$\begin{aligned} c_1 v_1(\gamma) + c_2 v_2(\gamma) &= 0 \\ c_1 v_1(\gamma) &= -c_2 v_2(\gamma) \\ v_1(\gamma) &= e v_2(\gamma) \quad e > 0 \end{aligned} \tag{3.26}$$

As we assumed that equation (3.25) holds for all γ, the equation (3.26) is only possible if $e = 1$ and $v_1 = v_2$, and this contradicts our valuations being distinct.

Rearranging equation (3.25) yields us

$$\begin{aligned} -c_1 v_1(\gamma) &= c_2 v_2(\gamma) + \cdots + c_m v_m(\gamma) \\ v_1(\gamma) &= d_2 v_2(\gamma) + \cdots + d_m v_m(\gamma) \quad \text{with } d_i = c_i/-c_1 \end{aligned} \tag{3.27}$$

in which at least one coefficient d_i is negative. Now we can apply our induction hypothesis to the right side of the equation 3.27. By our hypothesis, there exist elements $\alpha, \beta \in K$ so that for $2 \leq i \leq m$ we have

$$v_i(\alpha) = \begin{cases} 1, & \text{if } d_i \geq 0 \\ 0, & \text{if } d_i < 0 \end{cases} \quad \text{and } v_i(\beta) = \begin{cases} 0, & \text{if } d_i \geq 0 \\ 1, & \text{if } d_i < 0. \end{cases} \tag{3.28}$$

So α is an element that only picks the nonnegative coefficients d_i from equation (3.27), therefore $v_1(\alpha) \geq 0$. Likewise β only picks the negative coefficients, of which there is at least one, so $v_1(\beta) < 0$. Let us examine the sum $\alpha + \beta$. By the definition of valuations, because $v(\alpha) \neq v(\beta)$, then $v_i(\alpha + \beta) = min(v_i(\alpha), v_i(\beta)) = 0$ for each $i = 1, \ldots, m$. Therefore by equation 3.27 we have that $v_1(\alpha + \beta) = 0$. As v_1 is a valuation, we also have that $v_1(\alpha + \beta) = min(v_1(\alpha), v_1(\beta))$, and as we noted, $v_1(\beta) < 0$, so $v_1(\alpha + \beta) < 0$. We have arrived at a contradiction, and must conclude that our original assumption is wrong. □

Lemma 3.29. *[4] If L is a finite extension of degree n of a field K, then every valuation v_0 of the field K has at most n extensions to the field L.*

Proof. Let L be an extension of a field K and let v_0 be a valuation of K. Let $v_1, \ldots v_m$ be distinct extensions of v_0 into the field L. For every $1 \leq i \leq m$ consider the set of integers

$$z_i = \begin{cases} 1 & \text{if } j \neq i \\ 0 & \text{if } j = i \end{cases} \tag{3.30}$$

Then by Theorem 3.24 there exists an element $\gamma_i \in L$ for every i, so that

$$v_j(\gamma_i) = \begin{cases} 1 & \text{if } j \neq i \\ 0 & \text{if } j = i \end{cases} \tag{3.31}$$

What we now want to show is that the elements $\gamma_1, \ldots, \gamma_m$ are linearly independent in L, because if they are linearly dependent, then because L has a base with n elements over K, it would follow that $m > n$.

Let $\gamma \in L$ be a linear combination defined by

$$\gamma = a_1\gamma_1 + \cdots + a_m\gamma_m$$

where the coefficients $a_i \in K$ are not all zero. We need to prove that then $\gamma \neq 0$. To do this we are going to use our valuations to show that $v_k(\gamma)$ is finite for some k, and as such, γ can not be zero.

We start off by giving a lower bound for the coefficients a_i with respects to the valuation v_0. Define an integer

$$l = min(v_0(a_1), \ldots, v_0(a_m))$$

and let k be the index for which $v_0(a_k) = l$. Let e be the element used in the construction of the extension v_k, as seen in Lemma 3.22. By modifying the equation in Lemma 3.22, we get

$$v_k(\alpha) = ev_0(\alpha) \quad \text{for } \alpha \in L^*. \tag{3.32}$$

By using this equation, we get

$$\begin{aligned} v_k(a_k\gamma_k) &= v_k(a_k) + v_k(\gamma) \\ &= ev_0(a_k) + 0 = el \end{aligned}$$

and, for $j \neq k$, we get

$$\begin{aligned} v_k(a_j\gamma_j) &= v_k(a_j) + v_k(\gamma_j) \\ &= ev_0(a_j) + 1 \geq el + 1. \end{aligned}$$

From this and from the fact that $e > 0$, it follows that $v_k(a_j\gamma_j) > v_k(a_k\gamma_k)$ when $j \neq k$, so now we can represent a value for the valuation v_k at γ by

$$\begin{aligned} v_k(\gamma) &= v_k(a_1\gamma_1 + \cdots + a_m\gamma_m) \\ &= min(v_k(a_1\gamma_1, \ldots, a_m\gamma_m)) = el \end{aligned}$$

and as we noted earlier, as el is now a finite value, γ can not be zero. □

The next two theorems show that for a given valuation v_0, extensions to a finite field extension *exist*, and how we can construct the integral closure of the valuation ring D_{v_0} in L with the help of the valuation rings of all the extensions of v_0.

Theorem 3.33. *[4] Any valuation v_0 of a field K can be extended to any finite extension L of K.*

Proof. For a complete proof, see [4] □

Theorem 3.34. *[4] Let L be a finite extension of a field K, D_{v_0} be the ring of the valuation v_0 of a field K, and let D be the integral closure of D_{v_0} in a field L. For a set of all the valuations $v_1, \ldots, v_n$ that are extensions of the valuation v_0 to the field L, we have the following equality for the corresponding valuation rings $D_1, \ldots, D_n$ that*

$$D = \bigcap_{i=1}^{n} D_i$$

Proof. For a complete proof, see [4] □

The next theorem is going to give us the tools needed to prove the existence of a divisor theory for $\mathfrak{D}_K$, by proving that if we extend the valuations of a ring R in its quotient field, to some finite field extension, then the correspondingly extended valuations induce a divisor theory to the integral closure of the original ring R.

Theorem 3.35. *[4] Let the ring R with quotient field K have a divisor theory $f : R^* \to D$ which is induced by the set of valuations $\mathfrak{R}_0$ of K. If L is a finite field extension of K, then the set $\mathfrak{R}$ of all valuations in L, which are extensions of the valuations in $\mathfrak{R}_0$, determines a divisor theory for the integral closure $\mathfrak{D}$ of the ring R in the extension L.*

Proof. Theorem 3.14 gives us necessary and sufficient conditions for the set of valuations $\mathfrak{R}$ to determine a divisor theory. We then only need to verify that the set has all the necessary properties.

For any valuation $v \in \mathfrak{R}$ and any $a \in R$ it holds that $v(a) \geq 0$, for $v(a) < 0$ is possible only for the elements that are in the quotient field of R and not in the ring R itself. For such an element $a \in R$, by definition a is also an element of the ring $\mathfrak{D}_v$, and as we saw in Lemma 3.19, the valuation ring is integrally closed. This means that $\mathfrak{D} \subset D_v$, so $v(a) \geq 0$ for any $a \in \mathfrak{D}$ as well. For the other side of the argument, let $\alpha \in L$ be an element such that $v(\alpha) \geq 0$ for all $v \in \mathfrak{R}$. Let $x^r + a_1 x^{r-1} + \cdots + a_r$ be the minimal polynomial of α in K. Let $v_0 \in \mathfrak{R}_0$ be any valuation and let $v_1, \ldots, v_m$ (where $m \leq [L : K]$), be the extensions of v_0 into L. Now as we assumed $v_1(\alpha) \geq 0, \ldots, v_m(\alpha) \geq 0$, then by theorem 3.34 the element α is in the integral closure of D_{v_0} in L, which implies that the coefficients

of our minimal polynomial must lie in the ring D_{v_0}, so $v_0(a_i) \geq 0$ for all $i \leq r$. As this holds for all $v_0 \in \mathfrak{R}_0$, the coefficients a_i belong to R, so α belongs to $\mathfrak{D}$. We see that the second property holds true for $\mathfrak{R}$.

Next let $\alpha \in \mathfrak{D}$, $\alpha \neq 0$ and the minimal polynomial of α be defined as earlier. Then $v_0(a_r) = 0$ for all but a finite number of valuations $v_0 \in \mathfrak{R}_0$, because we assumed that the properties of theorem 3.14 hold for the set $\mathfrak{R}_0$. From the minimal polynomial of α we get the equation

$$\alpha^{-1} = -a_r^{-1}(\alpha^{r-1} + \cdots + a_{r-1})$$

which implies

$$\begin{aligned} v(\alpha^{-1}) &= v(-a_r^{-1}(\alpha^{r-1} + \cdots + a_{r-1})) \\ &= v(-a_r^{-1}) + v(\alpha^{r-1} + \cdots + a_{r-1})) \geq 0 \end{aligned}$$

As $v(\alpha^{-1}) = -v(\alpha)$ and because $\alpha \in \mathfrak{D}$ we have that $v(\alpha) \geq 0$ for almost all $v \in \mathfrak{R}$. It follows then, that $v(\alpha) = 0$ for almost all $v \in \mathfrak{R}$, and we have proven that the first condition holds.

On to the last condition. Let $v_1, \ldots, v_n$ be distinct valuations of $\mathfrak{R}$ and $z_1, \ldots, z_n$ be nonnegative integers. Let $v_{01}, \ldots, v_{0n}$ be the corresponding valuations in $\mathfrak{R}_0$. Next we expand the set of valuations to

$$v_1, \ldots, v_n, v_{n+1}, \ldots, v_m$$

containing all the expansions of the valuations v_{0i} to the field L. Theorem 3.24 states that there exists an element γ in the field L so that $v_1(\gamma) = z_1, \ldots v_n(\gamma) = z_n$ and $v_i(\gamma) = 0$ for $n < i \leq m$ If $\gamma \in \mathfrak{D}$ then set $\alpha = \gamma$ and we are done. Now assume $\gamma \notin \mathfrak{D}$ and denote by $v'_1, \ldots, v'_r$ the valuations in $\mathfrak{R}$ that have negative values in γ. In other words

$$v'_i(\gamma) = -l_i \quad \text{for nonnegative integers } l_i, \quad i \leq r$$

Again let $v'_{01}, \ldots, v'_{0r}$ be the corresponding valuations in $\mathfrak{R}_0$. Now the valuations v_{0i} are different from v'_{0j}, so there must be an element $a \in R$ so that

$$\begin{aligned} &v_{0i}(a) = 0 \quad (1 \leq i \leq m) \text{ and} \\ &v'_{0j}(a) = l \quad (1 \leq j \leq r) \quad l = max(l_1, \ldots, l_r) \end{aligned}$$

Now we can set $\alpha = \gamma a$ and observe that for all valuations v'_j

$$\begin{aligned} v'_j(\alpha) = v'_j(\gamma a) &= v'_j(\gamma) + v'_{0j}(a) \\ &= -l_i + l \geq 0 \end{aligned}$$

so $\alpha \in \mathfrak{D}$. We have proved the third condition required by theorem 3.14 and thus $\mathfrak{R}$ induces a divisor theory on the integral closure $\mathfrak{D}$ of R in the field L $\square$

Theorem 3.36. *[4] If $\mathfrak{D}_K$ is the maximal order of an algebraic number field K, then there exists a divisor theory $f : \mathfrak{D}_K \to D$ which is induced by the set $\mathfrak{R}_K$ of all valuations of K*

Proof. We shall apply theorem 3.35 to the case in hand. As the maximal order, $\mathfrak{D}_K$ is the integral closure of the ring $\mathbb{Z}$ in K. Since $\mathbb{Z}$ is a UFD, it has a divisor theory, one of which is induced by the set $\mathfrak{R}_{\mathbb{Q}}$ of all valuations of $\mathbb{Q}$.

Since every valuation of an algebraic number field is an extension of some valuation of $\mathbb{Q}$, it follows from theorem 3.35 that the set of valuations $\mathfrak{R}_K$ induces a divisor theory on the integral closure of $\mathbb{Z}$ in K, which is the maximal order $\mathfrak{D}_K$ □

Chapter 4

Dedekind rings, ramification of prime ideals

Building upon our newly constructed ring of integers for a given extension, we are going to begin exploring factorization over prime elements of our ring. In this case our primes are not going to be the prime numbers, but instead prime ideals.

Our original goal in the previous chapter was to regain unique factorization in some form for our number fields. We need to outline the properties necessary for this to happen at the ideal level. First off we require that our ring must be integrally closed, or to have a divisor theory, to stick with our standards of arithmetic in $\mathbb{Z}$.

We also need some assurance on whether the factorization is unique or not. The problem is that in our ring $\mathfrak{D}_K$ we might have prime ideals $P_1 \subset P_1'$, so we might be able to write the factorization with P_1' instead. This can be circumvented in the case where every prime ideal in our ring is uniquely contained, i.e. maximal.

Combining the above, we give the following definition for the rings that suit our goal.

Definition 4.1. [4, 5] We call a ring R a *Dedekind ring* if it has a divisor theory $f : R \to D$ and every prime ideal P of the ring R is maximal.

To prove that our maximal order $\mathfrak{D}_K$, the ring of integers is a Dedekind ring, the next lemma is our only missing piece.

Lemma 4.2. *[4, 5] Let K be an algebraic number field and $\mathfrak{D}_K$ its ring of integers. Let P be a prime ideal of $\mathfrak{D}_K$. Then $\mathfrak{D}_K/P$ is a field.*

Theorem 4.3. *Let K be an algebraic number field. Then $\mathfrak{D}_K$ is a Dedekind ring.*

Proof. By Theorem 3.36, $\mathfrak{D}_K$ has a divisor theory.

By Lemma 4.2 for any prime ideal P of $\mathfrak{D}_K$, $\mathfrak{D}_K/P$ is a field, therefore P is a maximal ideal in $\mathfrak{D}_K$.

We have shown that $\mathfrak{D}_K$ is a Dedekind ring. □

If we have a divisor theory $f : R \to D$ for a ring R, we can define for a given divisor $a \in D$ a set

$$\tilde{a} = \{\alpha \in R \mid a \mid f(\alpha)\}$$

which is an ideal of R. If $a \in D$ is a prime divisor, then $\tilde{a}$ is a prime ideal of R [5].

The following theorem shows that Dedekind rings have the necessary property we were after all along, namely unique factorization into prime ideals.

Theorem 4.4. *[4, 5] Let $f : R \to D$ be a divisor theory for a domain R and let $\tilde{a}$ be defined as above for $a \in D$. Then the map $a \to \tilde{a}$ is an isomorphism between the semigroup D and the semigroup of ideals of R.*

As the semigroup D in our divisor theory is a UFD, the isomorphism gives us the unique factorization of ideals into products of prime ideals in the Dedekind ring. Now prime divisors of D map to prime ideals of $\mathfrak{D}_K$, so when talking about prime divisors of $\mathfrak{D}_K$, we can just as well mean prime ideals.

Unfortunately we are not quite done in respects to our field K yet, as we have only constructed unique factorization for divisors of the ring $\mathfrak{D}_K$ so far. Next we expand our notion of a divisor to cover the whole field K. As our $\mathfrak{D}_K$ is the maximal order of K, $K = Quot(\mathfrak{D}_K)$ by definition. Therefore all valuations $v_p(x)$ of $\mathfrak{D}_K$ extend naturally to K as seen in Example (3.13). We can now extend our definition of a divisor as follows.

Definition 4.5. Let K be a number field and $\mathfrak{D}_K$ the maximal order. The expression

$$d = p_1^{e_1} \dots p_n^{e_n}$$

with prime divisors p_i of $\mathfrak{D}_K$ and integer exponents e_i are called *divisors* of K. If the exponents $e_i \geq 0$ for all i then d is a divisor of $\mathfrak{D}_K$ and we call it an *integral divisor*, otherwise it is called a *fractional divisor* [4].

As we saw in equation (3.15) the principal divisors can be defined by valuations, we can now extend this map to our field K by defining for all $\gamma = \alpha/\beta$ where $\alpha, \beta \in \mathfrak{D}_K$ that

$$f(\gamma) = f(\alpha/\beta) = \prod_p p^{v_p(\alpha) - v_p(\beta)} \quad \text{for all } \gamma \in K^*, \tag{4.6}$$

where p run through all the prime divisors of $\mathfrak{D}_K$ and $v_p(x)$ is the valuation for a prime divisor p. For $\gamma \in \mathfrak{D}_K$ the definition does not differ from equation (3.15) and $f(\gamma)$ is a

principal divisor of $\mathfrak{D}_K$. The divisors of the form (4.6) for some $\gamma \in K$ are called *principal divisors* of K.

We denote by $\tilde{D}$ the commutative group of all divisors of K. The map $f : K^* \to \tilde{D}$ defined above is a homomorphism from the multiplicative group of K^* to the group of divisors $\tilde{D}$ of K. For proofs of these claims see [4].

When speaking of divisibility in the field K, we must define what it means that a divisor of K divides some element $\alpha \in K$. This is very straightforward with valuations, as $\alpha \in K$ is divisible by a divisor

$$a = \prod_p p^{v_p(a)}$$

if $\alpha = 0$ or the principal divisor $f(\alpha)$ is divisible by a, meaning $v_p(\alpha) \geq v_p(a)$ for all valuations $v_p(x)$.

So if we already have an isomorphism between integral divisors and the nonzero ideals of $\mathfrak{D}_K$, could we also map fractional divisors to some sets related to $\mathfrak{D}_K$? The answer is yes, but we need to generalize our concept of an ideal, in relation to our field K.

Definition 4.7. Let K be a number field and $\mathfrak{D}_K$ its maximal order. A subset $A \subset K$ is called an *ideal of K in relation to $\mathfrak{D}_K$* if it has the following properties

- $(A, +)$ is a group,
- $\alpha A \subset A$ for any $\alpha \in \mathfrak{D}_K$, and
- there exists a $\beta \in K$ so that $\beta A \subset \mathfrak{D}_K$.

If $A \subset \mathfrak{D}_K$ then it is a regular ideal of $\mathfrak{D}_K$ and is called an *integral ideal*. Otherwise we call A a *fractional ideal*.

Finally we have the following theorem that gives us an isomorphism between all divisors of the field K and all of its generalized ideals.

Theorem 4.8. *[4] Let $\mathfrak{D}_K$ be a Dedekind ring with quotient field K. For every divisor a, denote by $\tilde{a}$ the set of all elements of K that are divisible by a. The map $a \to \tilde{a}$ is an isomorphism between all divisors of the field K and all the ideals of K. The map takes integral divisors to integral ideals, fractional divisors to fractional ideals, and vice versa.*

Proof. See [4] for proof. □

In an attempt to understand the unique factorization behavior we now define an equivalence relation for the divisors of K. We consider divisors to be equivalent if they only differ by a factor of a principal divisor. Here we mean principal divisors of K as defined in equation (4.6), not just of $\mathfrak{D}_K$ anymore.

Definition 4.9. [4] Let K be a number field, $\mathfrak{D}_K$ its ring of integers and f as in (4.6). We say that two divisors a and b of K are equivalent, if there exists an $\alpha \in K$ so that $a = f(\alpha)b$. We denote this by

$$a \sim b$$

and the equivalence class of a divisor a as $[a]$

Proposition 4.10. *[4] With the equivalence classes from Definition 4.9, we can define a multiplicative group structure by defining our multiplication as*

$$[a] \cdot [b] = [ab]$$

We call the group the divisor class group *or* ideal class group *as by Theorem 4.8 we have an isomorphism between ideals of K and divisors of K.*

Proof. The multiplication is well defined, because if $a \sim c$ and $b \sim d$, then by our definition we have $a = f(\alpha)c$ and $b = f(\beta)d$ which leads to the following

$$\begin{aligned} ab &= f(\alpha)cf(\beta)d \\ &= f(\alpha)f(\beta)cd \\ &= f(\alpha\beta)cd. \end{aligned}$$

The commutativity follows from our semigroup $\tilde{D}$ being commutative, and

$$f(a)f(b) = f(ab),$$

because f is a homomorphism. We have shown that the product does not depend on the choice of representatives.

The equivalence class [1] consists of only principal ideals. For any fractional we see that $[1][a] = [1a] = [a]$ so we have a neutral element in the group.

The product $[a][a^{-1}] = [aa^{-1}] = [1]$ shows that every class $[a]$ has an inverse $[a^{-1}]$ □

Definition 4.11. As a group, the divisor class group has an order, denoting the number of elements in the group. The order of the divisor class group of a number field K is called the *Class number* of K and is usually denoted as h_K.

The class number is one of the important invariants for algebraic number fields as it tells us how far from unique factorization the field is. If the field has class number 1, then it has unique factorization into primes.

Theorem 4.12. *[3] The class number for a number field K is always finite.*

Proof. See [4], [3] or [14] for a proof. □

We are going to introduce some more structures later on that are isomorphic to the ideal class group, and are in some cases easier to deal with. For this we need to refresh our knowledge on Galois theory in the next chapter. Before that, as the last part of this chapter, we introduce two definitions that describe the splitting of a prime of $\mathfrak{D}_K$ into primes in $\mathfrak{D}_L$.

Definition 4.13. Let K be a number field and p a prime ideal of $\mathfrak{D}_K$. Let L be a finite field extension of K and $\mathfrak{D}_L$ the ring of integers of L. Let us consider the product $p\mathfrak{D}_L$, which is now an ideal of $\mathfrak{D}_L$, but not necessarily prime. As L is a finite field extension of K, $p\mathfrak{D}_L$ must be a finite product of prime ideals P_i of $\mathfrak{D}_L$

$$p\mathfrak{D}_L = \prod_{i=1}^{g} P_i^{e_i}, \tag{4.14}$$

where g is the number of prime factors in the factorization. We call g the *decomposition number* of p. We say that p *ramifies* in L if the ramification index $e_i > 1$ for some i. If the ramification indices $e_i = 1$ for all i, then we say that p is *unramified* in L or that p *splits completely* in L.

Lastly we say that p is *totally ramified* in L if $e_i = [L : K]$ for some i.

We can also speak of ramification of a prime $P_i \subset \mathfrak{D}_L$, but in this case the ramification happens in relation to a prime $p \subset \mathfrak{D}_K$. A prime P_i ramifies over p if $e_i > 1$ and P_i is totally ramified over p if $e_i = [L : K]$.

Definition 4.15. Let K, L and p be as in (4.13) and let the factorization of $p\mathfrak{D}_L$ be as (4.14). The field $\mathfrak{D}_L/P_i$ is an extension of the field $\mathfrak{D}_K/p$ whenever P_i is a part of the factorization in (4.14). We define the *inertia degree* of P_i as the degree of the field extension

$$f_i = [\mathfrak{D}_L/P_i : \mathfrak{D}_K/p]$$

The inertia degree is in some sense a measure of how big of a gap in the 'coverage' between primes of $\mathfrak{D}_K$ and $\mathfrak{D}_L$ there is. The bigger the degree, the finer our factorizations become in $\mathfrak{D}_L$ compared to $\mathfrak{D}_K$.

Lastly we showcase a useful formula that applies for all algebraic number fields.

Proposition 4.16. *[14] Let K be an algebraic number field and L a finite extension and let g, f_i and e_i be the decomposition number, inertia degree and ramification index associated with a prime p of K and a prime P_i occurring in the factorization (4.14). the following holds for any prime p of K.*

$$[L : K] = \sum_{i=1}^{g} f_i e_i$$

Proof. For a complete proof see [14]. □

Chapter 5

Basic Galois Theory

In this chapter we are going to recall some of the general results of Galois theory for finite extensions, necessary for our later proofs. The most important being the connection between subgroups of our Galois group, and the corresponding sub-extensions of our number field extensions. We are also going to outline a Galois theory for algebraic extensions of infinite degree, and introduce a topology on this.

All of the following definitions work for infinite field extensions L/K as well.

Definition 5.1. Let L/K be an algebraic extension, $\alpha \in L$ and $f \in K[X]$ the minimal polynomial of α. We say that the minimal polynomial f is *separable* if it has $\deg f$ distinct roots in the algebraic closure of the field K.

If every element of a field L has a separable minimal polynomial, we say that the field L itself is separable extension.

Definition 5.2. An algebraic field extension L/K is called *Normal*, if every irreducible polynomial of $K[X]$ that has one root in L, has all its roots contained in L.

Definition 5.3. Let L/K be an algebraic field extension. We call this a *Galois extension*, or *Galois* for short, if it is a separable and normal extension.

Definition 5.4. Let L/K be a Galois extension. The Galois group of the field extension L/K is the group

$$Gal(L/K) = \{f \in Hom(L) \quad | \quad f(k) = k \quad \forall k \in K\}$$

Definition 5.5. Let L/K be a Galois extension. Let $H \subset Gal(L/K)$ be a subgroup. The set

$$L^H = \{l \in L \mid \sigma(l) = l \text{ for all } \sigma \in H\}$$

is called the *fixed field* of H.

Definition 5.6. [9] When we say that a field extension F in $K \subset F \subset L$ *corresponds* to a subgroup $H \subset Gal(L/K)$ we mean that $Gal(L/F) = H$ and $L^H = F$. Likewise a subgroup $H \subset Gal(L/K)$ *corresponds* to a field extension $F \subset L$ if $L^H = F$ and $Gal(L/L^H) = H$.

Now we can remind ourselves of the main theorem of Galois theory, concerning the subgroups of the Galois group, and the sub-field extensions of the field extension. The following theorem only holds when our field extension L/K is a finite Galois extension.

Theorem 5.7. *[9] Let L/K be a finite Galois extension. The correspondence defined in (5.6) between the fixed fields of the subgroups of $Gal(L/K)$, and the subfields $K \subset F \subset L$ is a bijection.*

Proof. See [9]. □

For the last chapter we need the following result that gives an isomorphism between products of Galois extensions and finite extensions.

Theorem 5.8. *[9] Let L/K be a Galois extension and let M/K be a finite extension. Then $Gal(ML/K) \cong Gal(L/L \cap M)$*

Proof. See [9]. □

We still require a similar correspondence in the case of infinite extensions, and this is what we will construct next. In the general case we need to require that our extension is at least algebraic, otherwise some elements might not have a minimal polynomial with respect to our field. Note that the following definitions will have a notion of an inverse limit as we have the inverse relation that for any field extension $K \subset F \subset L$ naturally $Gal(L/F) \subset Gal(L/K)$. So with a sequence $K_1 \subset K_2$.. we can talk about a limit for the Galois group, an inverse limit from the field extension perspective.

Even though in the previous chapter we had a very simple concept of the ramification of ideals in the case of algebraic number fields, in some instances we might end up with a ring of integers that is not a Dedekind domain. This can end up happening very easily in the case of field extension towers, where our field is given as a limit. Even in this case we need a working concept on what it means that an ideal ramifies. We achieve this through some structures on the Galois group of the extension.

From this point onward let L/K be an algebraic Galois extension. We start off by defining a *Krull topology* on our Galois group as follows.

Definition 5.9. [6] Let L/K be an algebraic Galois extension. Let F/K be a finite field extension such that $K \subset F \subset L$. Then $G_F = Gal(L/F)$ is of finite index in the group

$G = Gal(L/K)$. These G_F form a basis on $id \in G$, and by letting $\mathcal{F} = \{F_i\}$ be any family of finite Galois subextensions such that $\bigcup \mathcal{F} = L$, we get the following inverse limit

$$G \cong \lim_{\leftarrow} G/G_{F_i} \cong \lim_{\leftarrow} Gal(F_i/K)$$

where G_{F_i} are finite groups. These limits form a topology on our Galois group as our open sets.

Our Galois correspondence is the same as with finite extensions, except now we add topology on the side of galois groups. We do not yet know if the correspondence is bijective or not. The following theorem will tell us in which case it is a bijection.

Theorem 5.10. *[6, 9] For an algebraic Galois extension L/K there is a bijective correspondence between closed subgroups of $Gal(L/K)$ with regards to the Krull topology, and the intermediate field extensions $K \subset F \subset L$*

We need to introduce some vocabulary for the later sections. Let $K \subset L$ be our fields, p be a prime ideal of $\mathfrak{D}_K$ and P a prime ideal of $\mathfrak{D}_L$. We say that P *lies above* p if $P \cap \mathfrak{D}_K = p$.

Lemma 5.11. *[6] Let L/K be a Galois extension. Let P and P' be primes of L lying above a prime p of K. Then there exists a $\sigma \in Gal(L/K)$ so that*

$$\sigma(P) = P'$$

Proof. See [6] for a complete proof. □

As a reminder for the finite galois extension case, the inertia degrees and ramification indices for a prime p of K are all the same, so $f = f_1 = f_2 \ldots$ and $e = e_1 = e_2 \ldots$. Therefore for a Galois extension it holds that

$$[L : K] = efg,$$

where g is the decomposition number of a prime p (see [14] for a proof).

Definition 5.12. For a finite galois extension L/K and a prime $P \in \mathfrak{D}_L$ lying above a prime $p \in \mathfrak{D}_K$ we defined the *decomposition group* as

$$D = \{\sigma \in Gal(L/K) \mid \sigma(P) = P\}$$

and the *inertia group* as

$$I = \{\sigma \in Gal(L/K) \mid \sigma(P) \equiv P \mod P\}$$

The motivation for the Decomposition groups D and inertia groups I in the finite case was to be able to define the numbers f, e and g in different steps via field extensions.

For the decomposition group Z and the inertia group T it holds that we have a tower of field extensions $K \subset L^Z \subset L^T \subset L$ and

$$\begin{aligned} g &= [L^Z : K] \\ e &= [L : L^T] \\ f &= [L^T : L^Z] \end{aligned}$$

We want to extend our definitions of inertia and decomposition groups to the infinite Galois extensions. The way we achieve this is by using our definition for finite extensions, and a suitable series of finite Galois extensions that can be used to construct our infinite Galois extension. We end up constructing the final groups as the intersection of the intermediate groups.

If we have a prime $p \subset \mathfrak{D}_K$ and $P \subset \mathfrak{D}_L$ which lies above it, then as any automorphism $\sigma \in Gal(L/K)$ fixes K, it must also fix $\mathfrak{D}_K$ and so $\sigma(p) = p$. As an automorphism σ maps prime ideals to other prime ideals, so $\sigma(P) = P'$ for some other prime $P' \subset \mathfrak{D}_L$, which must then also lie above p. Lemma 5.11 proves the converse is also true, that we can always find an automorphism to shift one prime to another. We can therefore look at a subgroup of $Gal(L/K)$ that fixes a given prime P_i and if the subgroup is closed, our Galois correspondence (5.10) gives us a fixed field where this one prime is fixed.

Definition 5.13. Let p be a prime of K and P be a prime of L that lies above p. Let L/K be Galois. We define the *decomposition group* as

$$Z = Z(P/p) = \{\sigma \in Gal(L/K) \mid \sigma P = P\}$$

Lemma 5.14. *[6, 14] The decomposition group Z is closed.*

Proof. Let $K = F_0 \subset F_1 \cdots \subset F_n \cdots \subset L$ be a chain of fields such that each F_n/K is a finite Galois extension and $\bigcup F_n = L$. Define a set of primes by $p_n = P \cap \mathfrak{D}_{F_n}$. Next, let

$$Z_n = \{\sigma \in Gal(L/K) \mid \sigma(p_n) = p_n\}$$

For these sets it holds that $Z \subset Z_n$ for any n, and because $P = \bigcup p_n$, then $Z = \bigcap Z_n$.

Since $Gal(L/F_n) \subset Z_n$, Z_n it follows that $\sigma Gal(L/F_n) \subset Z_n$ for all $\sigma \in Z_n$, so every element of Z_n has an open neighborhood contained in Z_n, therefore Z_n is open. As Z_n is now open, σZ_n is also open for every $\sigma \in Gal(L/K)$, hence we can write

$$G \setminus Z_n = \bigcup_{\sigma \in G \setminus Z_n} \sigma Z_n$$

therefore Z_n is also closed, as a complement of an open set. As the intersection of closed sets, Z is closed. □

Now that we have a closed subgroup of our Galois group, our bijective Galois correspondence (5.10) says we have a unique fixed field $L^Z \subset L$. This fixed field is called the *decomposition field of* P in L/K and it has the property that it is the *smallest* intermediate field between K and L where P is the only prime above p

We extend our definition of the inertia group to the infinite Galois extension as follows.

Definition 5.15. [6, 14] Keeping to the same structures as previously, the *inertia group* is defined by

$$T = T(P/p) = \{\sigma \in Z \mid \sigma(\alpha) \equiv \alpha \mod P \text{ for all } \alpha \in \mathfrak{O}_L\},$$

where $\sigma(x) \equiv x \mod P$ is the regular definition for modulo ideals, so this is equivalent with $\sigma(x) - x \in P$

The inertia group is likewise closed, and we have a fixed field L^T, called the *inertia field of* P in L/K with the property that the inertia field is the *smallest* intermediate field between L and K where P is totally ramified.

For our later proofs we only require inertia groups, so the next part is presented only as a curiosity without proof, as to how inertia groups relate to ramification of a prime.

The ramification index could be defined with these for a given prime P of L as

$$e(P/p) =\mid T(P/p) \mid$$

in the case of Galois extensions. As before, P is totally ramified in L/K if

$$e(P/p) =\mid T(P/p) \mid= [L : K]$$

There exists a very useful structure in regards to what Galois theory has to offer, concerning field extensions. We give the following as a definition, but note that proof of existence and validity of the claim are still necessary. These fall under the domain of Class field theory.

Theorem 5.16. *[6] Let K be an algebraic number field and H its* maximal unramified Abelian extension. *Then*

$$Gal(H/K) \cong \textit{Ideal class group of } K$$

and $[H : K] = h_K =$ class number of K. We call the extension H the Hilbert class field.

Likewise for a given prime p, the fixed field of the p-sylow subgroup of $Gal(H/K)$ is the maximal unramified Abelian p-extension*, called the* Hilbert p-class field.

With this we should finally be well equipped to start exploring properties of infinite towers of field extensions. Our focus from the start has been to understand p-adic integers, so our next chapter will be outlining the structure and construction of the extension.

Chapter 6

Ring of p-adic integers, and $\mathbb{Z}_p$-extensions

In this chapter we consider some sequences of number fields with specific properties. Relating to the study of $\mathbb{Z}_p$-extensions, "inverse limits" inevitably pop up.

We start off by describing what we mean by the ring of $\mathbb{Z}_p$-integers. Recalling the definition for a valuation $v_p(x)$ from chapter 3, we can use this to define an absolute value on $\mathbb{Z}$ as follows and with it, also a metric. Thus $\mathbb{Z}$ becomes a topological ring.

Proposition 6.1. *For a p-adic valuation $v_p(x)$ of $\mathbb{Z}$ with $m > 1$, the map $|\cdot| : \mathbb{Z} \to [0, \infty[$*

$$|x| = m^{-v_p(x)}$$

defines an absolute value.

Proof. Let $x, y \in \mathbb{Z}$. Then

$$\begin{aligned} |x+y| = m^{-v(x+y)} &\leq m^{-min(v(x),v(y))} \text{ by the third property of valuations} \\ &\leq m^{-min(v(x),v(y))} + m^{-max(v(x),v(y))} \\ &= m^{-v(x)} + m^{-v(y)} \\ &= |x| + |y| \end{aligned}$$

For the absolute value of a product we have

$$\begin{aligned} |xy| &= m^{-v(xy)} \\ &= m^{-(v(x)+v(y))} = m^{-v(x)-v(y)} \\ &= m^{-v(x)} m^{-v(y)} = |x||y|. \end{aligned}$$

Lastly, for any x the absolute value is obviously positive, as we chose $m > 1$. What remains to be checked is when it is zero. If $|x| = 0$ then $m^{-n} = 0$, so $n \to \infty$. But $v(x) = \infty$ if and only if $x = 0$. □

As usual, given an absolute value map $|x|$ we can define a metric by $d(x, y) = |x - y|$. This gives our ring $\mathbb{Z}$ a topology. Note that the same maps also work for the field $\mathbb{Q}$.

Now that we have the concept of an absolute value, we can proceed the usual route of generating a completion for our ring $\mathbb{Z}$, where every Cauchy sequence converges. This will form our ring $\mathbb{Z}_p$

Definition 6.2. [9] By the completion of the set $\mathbb{Z}$, we mean the completion of the space $(\mathbb{Z}, |\cdot|)$, where $|\cdot|$ is as defined in (6.1). We denote this set by $\mathbb{Z}_p$ and call them the *p-adic integers.*

Proposition 6.3. *[10] Some of the more basic properties of $\mathbb{Z}_p$ consist of it being:*

- *an integral domain.*
- *a principal ideal domain.*
- *a topological ring.*
- *compact and complete.*

The topological properties of $\mathbb{Z}_p$ will be of great use to us later on. Note that by our construction of $\mathbb{Z}_p$, every element of it can be expressed as $\sum a_i p^i$, where $a_i \in \mathbb{Z}$. The finite sums are elements of $\mathbb{Z}$, which shows us that $\mathbb{Z} \subset \mathbb{Z}_p$

Definition 6.4. Let G be a multiplicative topological group. We call an element γ a *topological generator* if the set

$$B = \{1, \gamma, \gamma^2, \gamma^3, \dots\}$$

is dense in G with the given topology.

Lemma 6.5. *$1 \in \mathbb{Z}$ is a topological generator of $\mathbb{Z}_p$.*

Proof. As is well known, 1 generates $\mathbb{Z}$. The way we constructed $\mathbb{Z}_p$ implies that the closure $\bar{\mathbb{Z}}$ with regards to our metric yields $\mathbb{Z}_p$, hence $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. □

Definition 6.6. Let $K_0 \subset K_1 \subset \cdots \subset K_\infty$ be a sequence of number fields. The extension $K_\infty = \bigcup_{i=0}^{\infty} K_i$ is called a $\mathbb{Z}_p$-extension if for every $n \in \mathbb{N}$

$$Gal(K_n/K_0) \cong \mathbb{Z}/p^n\mathbb{Z},$$

as we then have the inverse limit for the Galois group of the extension K_∞/K_0

$$Gal(K_\infty/K_0) = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

The previous definition describes $\mathbb{Z}_p$-extensions as field extensions. Another way to define $\mathbb{Z}_p$-extensions with our ring of p-adic integers would be to say a field K_∞ is a $\mathbb{Z}_p$-extension if $Gal(K_\infty/K_0) \cong \mathbb{Z}_p$.

The following lemma gives some insight on the structure of K_∞ and the fields between K and K_∞. The basic idea is that there is a unique ascending chain of field extensions between K_∞ and K and their degrees are known powers of p.

Lemma 6.7. *[6] Let K_∞/K be a $\mathbb{Z}_p$-extension. Then, for each $n \geq 0$, there is a unique field K_n of degree p^n over K, and the only fields between K and K_∞ are these K_n and K_∞*

We finish off this chapter with two theorems that outline the ramification of primes in $\mathbb{Z}_p$-extensions.

Theorem 6.8. *[6] Let K_∞ be a $\mathbb{Z}_p$-extension and let $\hat{l}$ be a prime of K that does not lie above p. Then K_∞/K is unramified at $\hat{l}$. This means that $\mathbb{Z}_p$-extensions are unramified outside p.*

Theorem 6.9. *[6] Let K_∞ be a $\mathbb{Z}_p$-extension. At least one prime of K ramifies in this extension, and there exists $n \geq 0$ so that every prime of K_n which ramifies in K_∞ is totally ramified.*

Proof. As K is a number field, its class number is finite. Therefore the Hilbert class field is also a finite extension, and as this is the maximal unramified abelian extension of K, it is merely a subfield of K_∞, so some prime must ramify in K_∞/K.

By the previous lemma and because only a finite amount of primes P of K can lie above $p \in \mathbb{Z}$, only a finite number of primes of K ramify in K_∞/K. Let these primes be $p_1, \ldots, p_l$ and let $I_1, \ldots I_l$ be their inertia groups. As the inertia groups are closed subgroups in our topology, the intersection is also a subgroup and because the closed subgroups of $\mathbb{Z}_p$ are all of the form $p^n\mathbb{Z}_p$, we must have the following

$$\bigcap I_j = p^n\mathbb{Z}$$

for some $n \geq 0$. By lemma 6.7 the fixed field of $p^n\mathbb{Z}_p$ is K_n so $Gal(K_\infty/K_n) \subset I_j$ for all $1 \leq j \leq l$. This also means that the fixed fields of I_j are subfields of K_∞/K, and because the fixed field of an inertia group is the smallest intermediate field where the prime in question is totally ramified, then all of our primes $p_1, \ldots p_l$ are totally ramified in K_∞/K. □

Chapter 7

Λ-modules

In this chapter we shall be constructing a ring structure of formal power series of our $\mathbb{Z}_p$-extension. The elements of the ring are going to consist of polynomials of possibly infinite length, that we are only going to be using as sequences with a ring structure.

We start off with a multiplicative topological group Γ, generated by an element γ and isomorphic to the additive group of our p-adic integers $\mathbb{Z}_p$. The two groups are then isomorphic by the map $x \mapsto \gamma^x$.

Let $\Gamma_n = \Gamma/\Gamma^{p^n}$. Then $\Gamma_n \simeq \mathbb{Z}/p^n\mathbb{Z}$ is cyclic of order p^n. Now let us consider the group rings (see 2.14) of Γ_n over $\mathbb{Z}_p$, denoted as $\mathbb{Z}_p[\Gamma_n]$. As $\Gamma_n \subset \Gamma_m$ for all $m > n > 0$, and as both are cyclic, there is a natural map $\phi'_{m,n} : \Gamma_m \to \Gamma_n$ that induces a map ([6][13])

$$\phi_{m,n} : \mathbb{Z}_p[\Gamma_m] \to \mathbb{Z}_p[\Gamma_n]$$

Lemma 7.1. *[6] The isomorphism $\mathbb{Z}_p[\Gamma_n] \simeq \mathbb{Z}_p[T]/((1+T)^{p^n} - 1)$ is defined by*

$$\gamma \mod \Gamma^{p^n} \to 1 + T \mod ((1+T)^{p^n} - 1)$$

Proof. See [6]. □

With these, the following diagram commutes

$$\begin{array}{ccc} \mathbb{Z}_p[\Gamma_{n+1}] & \xrightarrow{7.1} & \mathbb{Z}_p[T]/((1+T)^{p^{n+1}} - 1) \\ \downarrow{\scriptstyle \phi_{n+1,n}} & & \downarrow \\ \mathbb{Z}_p[\Gamma_n] & \xrightarrow{7.1} & \mathbb{Z}_p[T]/((1+T)^{p^n} - 1) \end{array}$$

From the diagram we can see that there exists a limit for the Γ_n that we can denote as $\mathbb{Z}_p[[\Gamma]] = \lim \mathbb{Z}_p[\Gamma_n]$. Based on our diagram, this *profinite group ring* of Γ over $\mathbb{Z}_p$ can also be seen as a limit on polynomial rings, as

$$\mathbb{Z}_p[[\Gamma]] \simeq \lim_{\leftarrow} \mathbb{Z}[T]/((1+T)^{p^n} - 1)$$

Theorem 7.2. *[6][13] The isomorphism $\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$ is induced by the map $\gamma \to 1+T$*

Proof. See [13]. □

We call the limit $\Lambda = \lim \mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[[T]]$ the *Iwasawa Algebra*
Now we can define a module over Λ as follows.

Definition 7.3. Let Λ, Γ and Γ_n be as before. Let V_n be a module over $\mathbb{Z}_p[\Gamma_n]$ and let us have module homomorphisms $V_{n+1} \to V_n$ for every n. We call the limit

$$V = \lim V_n$$

a Λ-*module*.

Definition 7.4. We say that a polynomial $P(T) \in \Lambda$ is *distinguished* if for

$$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$$

our prime p divides all the coefficients a_i.

The p-adic Weierstrass preparation theorem (see [6] for details) states that any nonzero polynomial $f(T) \in \Lambda$ can be uniquely written as

$$f(T) = p^\mu P(T)U(T)$$

where $\mu > 0$, $P(T) \in \Lambda$ is distinguisted and $U(T) \in \Lambda$ is a unit of Λ.

Definition 7.5. [6] Two Λ-modules M and M' are called *pseudo-isomorphic* if there exists a homomorphism $f : M \to M'$ for which both $\ker f$ and $co\ker f = M'/Imf$ are finite Λ-modules. We denote this as

$$M \sim M'$$

This means that we have an exact sequence

$$0 \to A \to M \to M' \to B \to 0$$

where A and B are finite Λ-modules.

The next theorem will become useful in our next chapter after we prove that a specific Galois group as a Λ-module is finitely generated, as the theorem lets us split the module into direct sums of quotients generated by ideals and distinguished polynomials of Λ.

Theorem 7.6. *[6] Let M be a finitely generated Λ-module. Then*

$$M \sim \Lambda^r \oplus (\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})) \oplus (\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j}))$$

where $r, s, t, n_i, m_j \in \mathbb{Z}$ and the polynomials f_j are distinguished and irreducible.

Chapter 8

Iwasawa theory

The main goal of this final chapter is to introduce the results of Iwasawa on the class number of $\mathbb{Z}_p$-extensions, specifically what happens with the class number of each K_n in the tower of extensions, and showing that there exist invariants that make defining the class number easy for sufficiently large n. The whole chapter will be closely following the proof given in [6], filling in the gaps to the best of my ability.

For the whole chapter we shall be working with the following structures. Working off the results of our last chapter, let our multiplicative group be

$$\Gamma = Gal(K_\infty/K) \cong \mathbb{Z}_p$$

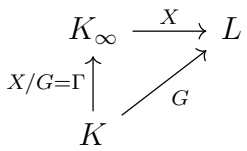
and let γ_0 be the topological generator of Γ as defined in 6.5. Let L_n be the maximal abelian unramified p-extension of K_n(in other words, the Hilbert p-class field of K_n), and $X_n = Gal(L_n/K_n) \cong A_n$, which is p-Sylow of the ideal class group of K_n [6]. Because each L_n is maximal, they are Galois over K, so the set $L = \bigcup_{i\geq 0} L_i$ is also Galois. Let $X = Gal(L/K_\infty)$ as limits of X_n and $G = Gal(L/K)$.

Lastly note that the quotient

$$G/X = Gal(L/K_\infty)/Gal(K_\infty/K) = \Gamma$$

because for any two morphisms $\alpha \in G$ and $\beta \in X$, the composition $\alpha\beta$ does belong to $Aut(L)$, but it only fixes the smaller of the two base fields, hence $\alpha\beta \in \Gamma$.

We have the following diagram for the relations of our Galois groups, where the direction of arrows points to the field extension, and the labels are the corresponding Galois groups.



For the next lemmas we will be using the following assumption:
Assumption: *Assume that all primes of K_∞/K which are ramified, are totally ramified.* This assumption is not completely unfounded, as we saw in Theorem 6.9 that at least one prime ramifies in K_∞/K and there exists a $n \geq 0$ so that every prime that ramifies in K_∞/K_n is totally ramified. Later on we will start working off a lower bound $e \geq 0$ and a field K_e instead of K_0.

We know that some prime P of K must ramify in K_∞ as the maximal unramified extension of K is finite. By our assumption P is then also totally ramified in K_∞. Note that as the prime P totally ramifies in K_∞/K it also totally ramifies in any subextension M/L_0 that is between K_∞ and the maximal unramified p-extension L_0 of K, i.e.

$$K \subset L_0 \subset M \subset K_\infty$$

As $K_n \subset K_{n+1}$ and also $K_n \subset L_n$, the intersection $K_{n+1} \cap L_n$ is a field extension of K_n. Note also that the maximal unramified p-extension L_0 of K is contained in every L_n. Therefore we have the following inclusions

$$K \subset L_0 \subset K_n \subset K_{n+1} \cap L_n \subset K_\infty$$

so P is totally ramified in $K_{n+1} \cap L_n/K_n$. On the other hand L_n/K_n is by definition unramified for all primes, so as $K_n \subset K_{n+1} \cap L_n \subset L_n$ it means that the sub-field extension $K_{n+1} \cap L_n/K_n$ must also be unramified (we can not have a totally ramified prime in a sub-extension that is contained in an unramified extension). The only way the extension $K_{n+1} \cap L_n/K_n$ can at the same time be unramified, and totally ramified at P, is if it is a trivial extension $K_{n+1} \cap L_n/K_n = K_n/K_n$. Thus we have that

$$K_{n+1} \cap L_n = K_n$$

therefore by theorem 5.8 we have

$$\begin{aligned} Gal(L_nK_{n+1}/K_{n+1}) &\cong Gal(L_n/K_{n+1} \cap L_n) \\ &= Gal(L_n/K_n) \\ &= X_n \end{aligned}$$

As $Gal(K_{n+1}L_n/K_{n+1})$ is a quotient of X_{n+1}, we thus have a map from $X_{n+1} \to X_n$(which is in effect the norm map on ideal class groups [6]).

Before we get to the theorems, we still need to construct our Λ-module, and note some useful identities for the Galois groups. We have the necessary projections, now we only need to show that as a limit of X_n we actually get our defined X. As

$$\begin{aligned} X_n &= Gal(L_n/K_n) \\ &\cong Gal(L_nK_{n+1}/K_{n+1}) \dots \\ &\cong Gal(L_nK_l/K_l) \dots \cong Gal(L_nK_\infty/K_\infty) \end{aligned}$$

so we get that

$$\lim_{\leftarrow} X_n \cong Gal((\bigcup L_n K_\infty)/K_\infty) = Gal(L/K_\infty) = X$$

Now we have our group Γ and X, but we still need to make X into a Λ-module to be able to utilize our previous results. We do this by defining an action on the group as follows. Let $\gamma \in \Gamma/\Gamma^{p^n}$. We extend γ to $\tilde{\gamma} \in Gal(L_n/K)$ and let it act on $x \in X_n$ by conjugation

$$x^\gamma = \tilde{\gamma} x (\tilde{\gamma})^{-1}$$

The action is well defined for every n, as our groups $Gal(L_n/K_n)$ are abelian by definition. Thus X_n is a $\mathbb{Z}_p[\Gamma_n]$-module. We still need to show that every $x^\gamma \in X$ to be able to conclude that X is a Λ-module. Let us consider an $x \in X$ as a vector

$$x = (x_i) \quad x_i \in X_i$$

and let our action be defined as before, for each X_i separately. Then we can extend our action so x^γ for our vector means γ acts on the nth coordinate accordingly. We see that

$$\tilde{\gamma} x_i (\tilde{\gamma})^{-1} \in X_i$$

so our vector stays intact, and therefore $x \in X$

Lastly we introduce a useful representation for our group G by means of inertia groups. The polynomial $1 + T \in \Lambda$ acts as our generator $\gamma_0 \in \Gamma$, and with that we have

$$x^\gamma = \tilde{\gamma} x \tilde{\gamma}^{-1} \quad \text{for } \gamma \in \Gamma, x \in X$$

where, as earlier $\tilde{\gamma}$ is the extension of γ.

We know from earlier lemmas that only finitely many primes ramify in K_∞/K, so let us denote these as $p_1, \ldots, p_s$. Next we fix a prime $\tilde{p_i} \in L$ lying above p_i and let $I_i \subset G$ be the corresponding inertia group. Since L/K_∞ is unramified because all our L_n are unramified, the following holds

$$I_i \cap X = 1$$

Due to our assumption, K_∞/K is totally ramified at p_i, so

$$I_i \hookrightarrow G/X$$

is surjective, thus bijective[6]. This means that we have the identity

$$G = I_i X = X I_i \quad i = 1, \ldots, s$$

Now let $\sigma_i \in I_i$ map to our generator $\gamma_0 \in \Gamma$. As γ_0 was the topological generator of Γ, it must be that σ_i is a topological generator of our inertia group I_i. Also note that since $I_i \subset XI_1$ for all i, then

$$\sigma_i = a_i \sigma_1$$

for some $a_i \in X$.

Lemma 8.1. *[6] With our assumption, let G' be the closure of the commutator subgroup of G. Then*

$$G' = X^{\gamma_0 - 1} = TX$$

Proof. As was noted earlier, $\Gamma \cong I_1 \subset G = \Gamma X$, so we proceed by lifting the elements $\gamma \in \Gamma$ with the isomorphism to an element of I_1, in order to define an action of Γ on X. Let our action be as before

$$x^\gamma = \gamma x \gamma^{-1}$$

where our γ is now lifted.

Let us take two arbitrary elements from ΓX. Let $a = \alpha x$ and $b = \beta y$ where $\alpha, \beta \in \Gamma$ and $x, y \; inX$. Let us rework the commutator $aba^{-1}b^{-1}$

$$\begin{aligned}
aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \quad \text{replace with } ax = axa^{-1}a = x^a a \\
&= x^\alpha \alpha \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \quad \text{replace with } \alpha\beta y x^{-1} = (yx^{-1})^{\alpha\beta}(\alpha\beta) \\
&= x^\alpha (yx^{-1})^{\alpha\beta} (\alpha\beta) \alpha^{-1} y^{-1} \beta^{-1} \quad \text{as } \Gamma \text{ is abelian, we get } (\alpha\beta)\alpha^{-1} = (\beta\alpha)\alpha^{-1} = \beta \\
&= x^\alpha (yx^{-1})^{\alpha\beta} \beta y \beta^{-1} \\
&= x^\alpha (yx^{-1})^{\alpha\beta} (y^{-1})^\beta \\
&= x^\alpha x^{-\alpha\beta} y^{\alpha\beta} y^{-\beta} \\
&= (x^\alpha)^{1-\beta} (y^\beta)^{\alpha - 1}
\end{aligned}$$

For all of the above steps we required the lifting of α, β into X in order to work with them as regular exponents.

Now we use the result as follows. First let $\beta = 1$ and $\alpha = \gamma_0$, then we have that

$$x^0 y^{\gamma_0 - 1} = y^{\gamma_0 - 1} \in G'$$

so $X^{\gamma_0 - 1} \subset G'$

Next we note that for arbitrary β, there exists a $c \in \mathbb{Z}_p$ so that $\beta = \gamma_0^c$, as γ_0 was our topological generator. Remember that with Λ-modules, our generator γ_0 maps to

$1 + T \in \Lambda$, so we have

$$\begin{aligned} 1 - \beta =& 1 - \gamma_0^c \\ =& 1 - (1+T)^c \\ =& 1 - \sum_{i=0}^{\infty} \binom{c}{i} T^i \\ =& 1 - \sum_{i=0}^{\infty} \frac{c(c-1)\cdots(c-i+1)}{i!} T^i \in T\Lambda \end{aligned}$$

because $\binom{c}{i} \in \mathbb{Z}_p$ when $c \in \mathbb{Z}_p$ (see [6] chapter for p-adic functions).

As $\gamma_0 - 1 = T$, this implies that $X^{\gamma_0 - 1} = TX$ and we get that $(x^\alpha)^{1-\beta} \in X^{\gamma_0 - 1}$. Proceeding in the same fashion, also $(y^\beta)^{\alpha - 1} \in X^{\gamma_0 - 1}$.

Since $TX = X^{\gamma_0 - 1}$ is the image of the compact set X, it is closed. We just showed that all commutators belong to TX, therefore $G' \subset X^{\gamma_0 - 1}$ as well. This proves our claim. □

The next lemma will prove to be very useful in transferring properties of X_n to properties of X, especially when proving later on that X is finitely generated. Note that in the lemma we create submodules by taking sums of the generator element γ_0 and multiplying by a base $\mathbb{Z}_p$-submodule Y_0. The sum

$$v_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n - 1}$$

can be shortened by the regular sum formula for geometric series, which gives us

$$v_n = \frac{\gamma_0^{p^n} - 1}{\gamma_0 - 1} \cong \frac{(1+T)^{p^n}}{1 + T - 1}$$

where the isomorphism with the polynomial follows from our isomorphism $\gamma_0 \to 1 + T$.

Lemma 8.2. *[6] With our assumption, Let Y_0 be the $\mathbb{Z}_p$-submodule of X generated by $\{a_i \mid 2 \le i \le s\}$, where a_i are as mentioned before and by $X^{\gamma_0 - 1} = TX$. Let $Y_n = v_n Y_0$, where*

$$v_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n - 1} = \frac{(1+T)^{p^n} - 1}{T}$$

Then

$$X_n \simeq X / Y_n \quad \text{for } n \ge 0$$

Proof. See [6]. □

Lemma 8.3. *[6] (Nakayama's Lemma) Let X be a compact Λ-module. Then*

$$X \text{ is finitely generated over } \Lambda \Leftrightarrow X/(p,T)X \text{ is finite .}$$

If $x_1, \ldots, x_n$ generates $X/(p,T)X$ over $\mathbb{Z}$, then they also generate X as a Λ-module. Especially the following holds:

$$X/(p,T)X = 0 \Leftrightarrow X = 0$$

Proof. See [6]. □

Lemma 8.4. *[6] With our assumption still in place, $X = Gal(L/K_\infty)$ is a finitely generated Λ-module.*

Proof. Our proof will utilize lemma 8.2 heavily. We start off by noting that

$$v_1 \in (p,T)$$

because (p,T) is the maximal ideal of Λ generated by p and T. Then $Y_0/(p,T)Y_0$ is a quotient of Y_0/v_1Y_0 which by our definition of Y_n is the same as $Y_0/Y_1 \subset X/Y_1 \cong X_1$. As X_1 is finite, this means that Y_0/Y_1 must also be finite, and because $Y_1 = v_1Y_0$ it follows from lemma 8.3 that Y_0 must be finitely generated.

Now then, because X_0 is also finite, and $X_0 \cong X/Y_0$ by lemma 8.2, the quotient must also be finite. As we showed that X/Y_0 is finite, it follows from lemma 8.3 that X must also be finitely generated.

□

Now we move on to the more general case, for arbitrary K. We still work with a $\mathbb{Z}_p$-extension K_∞/K. From now on we will only be dealing with K_e where $e \geq 0$ has been chosen as in theorem 6.9. Our earlier results are still valid, as now the original assumption still holds starting from our field K_e.

Lemma 8.5. *[6] Let K_∞/K be a $\mathbb{Z}_p$-extension. Then X is a finitely generated Λ-module and there exists an $e \geq 0$ so that*

$$X_n \simeq X/v_{n,e}Y_e \quad \text{for all } n \geq e$$

Proof. Choose a $e \geq 0$ so that all primes which are ramified in K_∞/K_e are totally ramified. Note that for the extensions K_∞/K and K_∞/K_e our $X = Gal(L/K_\infty)$ stays the same. By lemma 8.4 X is a finitely generated Λ-module.

Since $\gamma_0^{p^e}$ generates $Gal(K_\infty/K_e)$, we can rewrite our v_e from lemma 8.2 as

$$v_{n,e} := 1 + \gamma_0^{p^e} + \gamma_0^{2p^e} + \cdots + \gamma_0^{p^n - p^e} = \frac{v_n}{v_e} \tag{8.6}$$

Using $v_{n,e}$ in place of v_n for Y_e in lemma 8.2, let $Y_n = v_{n,e}Y_e$. The assumptions of the lemma hold as we can replace Y_0 by Y_e. Therefore by lemma 8.2 our claim holds. □

As we have proven that X is a finitely generated Λ-module, we can apply theorem 7.6 to X and get that X is a direct sum of Λ-modules of the form Λ^r, $\bigoplus \Lambda/(p^{k_i})$ and $\bigoplus \Lambda/(f(T)^{m_j})$.

Proposition 8.7. *[6] Suppose*

$$E = \Lambda^r \oplus (\bigoplus_{i=1}^{s} \Lambda/(p^{k_i})) \oplus (\bigoplus_{j=1}^{s} \Lambda/(g_j(T)))$$

where each $g_j(T)$ is distinguished *but not necessarily irreducible. Let $m = \sum k_i$ and $l = \sum deg(g_j)$. If $E/v_{n,e}E$ is finite for all n, then $r = 0$ and there exist n_0 and c such that*

$$| E/v_{n,e}E | = p^{mp^n+ln+c} \quad \text{for all } n \geq n_0$$

Proof. See [6]. □

We now have an *exact sequence*

$$0 \to A \to Y_e \to E \to B \to 0$$

where A and B are finite and E is as defined in proposition 8.7. The order of $E/v_{n,e}E$ is known to us for all $n \geq n_0$, but we still need similar information on Y_e. At this point we can only conclude that $e_n = mp^n + ln + c_n$ where c_n is bounded.

The next lemma will solve our problem with c_n being dependent on n

Lemma 8.8. *[6] Suppose Y and E are Λ-modules with $Y \sim E$ such that $Y/v_{n,e}Y$ is finite for all $n \geq e$. Then for some constant c, and some n_0*

$$| Y/v_{n,e}Y | = p^c \mid E/v_{n,e}E \mid \quad \text{for all } n \geq n_0$$

Proof. see [6] for specifics, but also a book on homological algebra for the *Snake Lemma* that is used to construct a long exact sequence from the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & v_{n,e}Y & \longrightarrow & Y & \longrightarrow & Y/v_{n_e}Y & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'_n} & & \downarrow{\scriptstyle \phi'} & & \downarrow{\scriptstyle \phi''} & & \\ 0 & \longrightarrow & v_{n,e}E & \longrightarrow & E & \longrightarrow & E/v_{n,e}E & \longrightarrow & 0 \end{array}$$

□

By combining our previous results all together, we get the following theorem of Iwasawa.

Theorem 8.9. *[6] (Iwasawa's Theorem) Let K_∞/K be a $\mathbb{Z}_p$ extension. Let p^{e_n} be the exact power of p dividing the class number of K_n Then there exist integers $\lambda \geq 0$, $\mu \geq 0$ and v, all independent of n, and an integer n_0 so that*

$$p^{e^n} = p^{\lambda n+\mu p^n+v} \quad \text{for all } n \geq n_0$$

Proof. Let E be as defined in 8.7. Then as the fields used for X_n are p-extensions, the p-part of the class number h_{K_n} is $\mid X_n \mid$.

From theorems 8.2 and 8.5, we know that there exists an $e \geq 0$ so that

$$\mid X_n \mid = \mid X/v_{n,e}Y_e \mid$$

Now note that $X/v_{n,e}Y_e$ is a finite quotient, so we can count the order by splitting Y_n into a partition itself over Y_e, and taking the product of the orders, therefore

$$\mid X/Y_n \mid = \mid X/Y_e \mid\mid Y_e/v_{n,e}Y_e \mid$$

where $\mid X/Y_e \mid$ does not depend on n, so it is a constant that divides p^{e_n}.

As E was such a module that $Y_e \sim E$ and $Y_e/v_{n,e}Y_e$ is finite for all $n \geq e$, then by lemma 8.8 there exist some constants n_0, c so that $\mid Y_e/v_{n,e}Y_e \mid = p^c \mid E/v_{n,e}E \mid$ for all $n \geq n_0$.

By lemma 8.7 we know that there exist constants μ, λ, c, n_0 so that

$$\mid E/v_{n,e}E \mid = p^{\mu p^n + \lambda n + c} \quad \text{for all } n \geq n_0$$

Combining all of our results together gives us

$$\begin{aligned} p^{e^n} = \mid X_n \mid &= \mid X/Y_e \mid\mid Y_e/v_{n,e}Y_e \mid \\ &= (constant) \mid E/v_{n,e}E \mid \\ &= p^{\lambda n + \mu p^n + v} \quad \text{for all } n \geq n_0 \end{aligned}$$

□

Bibliography

[1] Tauno Metsänkylä, Marjatta Näätänen: Algebra, Limes, 2003

[2] Jokke Häsä: Algebra II, luentomoniste, Helsingin yliopisto, 2010.

[3] Serge Lang, Algebra, Springer, 2002.

[4] Borevich, Shafarevich, Academic Press, 1966.

[5] Helmut Koch: Algebraic Number Theory, Springer, 1997.

[6] Lawrence C. Washington: Introduction to Cyclotomic Fields, Springer, 1997.

[7] Serge Lang, Cyclotomic Fields I and II, Springer, 1990.

[8] Harvey Cohn, A Classical Invitation to Algebraic Numbers and Class Fields, Springer, 1978.

[9] P. M. Cohn: Algebra volume 2, John Wiley & Sons Ltd., 1977.

[10] Alain M. Robert: A Course in p-adic analysis, Springer, 2000.

[11] Kenkichi Iwasawa: Lectures on p-adic L-functions, Princeton University Press, 1972.

[12] Kurt Mahler: Introduction to p-adic numbers and their functions, Cambridge University Press, 1973.

[13] Serge Lang: Cyclotomic Fields, Springer, 1978.

[14] Paulo Ribenboim: Classical Theory of Algebraic Numbers, Springer, 2001.

[15] Serge Lang: Algebraic Number Theory, Springer, 1986.

[16] Kenneth S. Brown: Cohomology of Groups, Springer, 1982.